



# אסטרטגיית סייבר לאומית: סוגיות לדיון

שי שבתאי



עיונים בביטחון המזרח התיכון מס' 203

---

אוניברסיטת בר-אילן  
עיונים בביטחון המזרח התיכון מס' 203

## אסטרטגיית סייבר לאומית: סוגיות לדין

שי שבתאי

**אסטרטגיית סייבר לאומית: סוגיות לדין**

**National Cyber Strategy: Issues for Discussion**

Shai Shabtai

מרכז בגין-סאדאת למחקרים אסטרטגיים (בס"א)  
אוניברסיטת בר-אילן  
רמת גן 5290002  
טל' 03-5318959  
[besa.center@biu.ac.il](mailto:besa.center@biu.ac.il)

ISSN 0793-1042

**ינואר 2024**

© כל הזכויות שמורות  
תמונת שער: shutterstock

## מרכז בגין-סאדאת (בס"א) למחקרים אסטרטגיים

---

מרכז בגין-סאדאת למחקרים אסטרטגיים (מרכז בס"א) עורך מחקרים מכווני מדיניות בנושאים אסטרטגיים - במיוחד בנושאים הקשורים לביטחון הלאומי של ישראל ולמדיניות החוץ שלה - ובסוגיות אזוריות במזרח התיכון.

פרסומיו של מרכז בס"א מכוונים אל מקבלי ההחלטות הישראלים הבכירים במערכת הפוליטית, במסד הביטחוני ובשירות החוץ של ישראל, וכן אל הסגל הדיפלומטי, התקשורת, הקהילה האקדמית, מנהיגי הקהילות היהודיות ברחבי העולם והקהל המשכיל באופן כללי.

המרכז מקיים כנסים בין-לאומיים, הרצאות ותדרוכים המיועדים לקהל בין-לאומי ומקומי. באירועים אלה משתתפים מומחים מובילים בתחומם מן האקדמיה ואנשי מעשה מהארץ ומחו"ל. מרכז בס"א פיתח שיתופי פעולה פוריים עם מכונים מובילים בתחום המחקר האסטרטגי בכל רחבי העולם.

## ועד מנהל

---

פרופ' אמנון אלבק, פרופ' גיל אפשטיין, פרופ' רמי גינת, פרופ' יהושע טייטלבוים, פרופ' ג'ונתן ריינהולד, פרופ' איתן שמיר.

## צוות המרכז

---

מנהל המרכז: פרופ' איתן שמיר  
חוקרים: ד"ר אפרת אביב, ד"ר שי אטיאס, סא"ל (מיל) ד"ר רפאל בוכניק-חן, ד"ר זיו בורר, ד"ר יעלי בלוך-אלקון, סא"ל (מיל) ד"ר שאול ברטל, אלוף (מיל) גרשון הכהן, ד"ר עדו הכט, השגריר מיכאל הררי, תא"ל (מיל) ד"ר מוני חורב, פרופ' יהושע טייטלבוים, פרופ' אודי לבל, ד"ר אלון לבקוביץ, סא"ל (מיל) דוד לוי, ד"ר יוסף מן, פרופ' שמואל סנדלר, פרופ' יונתן פאקס, ד"ר אייל פינקו, ד"ר נתנאל פלמר, פרופ' אפרים קארש, ד"ר עוזי רובין, ד"ר אלישבע רוסמן, ד"ר עילי רטיג, פרופ' יונתן ריינהולד, אל"מ (מיל) שי שבתאי, מרן שגב, סא"ל (מיל) ד"ר דני שוהם, פרופ' שלמה שפירא.

מרכזת: אלונה ברינר

מנהלת משרד ושיווק דיגיטאלי: שני שריקי

עריכה באנגלית: יהודית לוי

# אסטרטגיית סייבר לאומית: סוגיות לדיון

שי שבתאי

## עיקרי הדברים

אחד מיעדי תוכנית העבודה השנתית של מערך הסייבר הלאומי לשנת 2023 טרם פרוץ המלחמה היה גיבוש האסטרטגיה הלאומית להגנת הסייבר ובניית תוכנית עבודה רב-שנתית. תהליך הגיבוש של אסטרטגיה זו נמשך חודשים רבים.

מטרת המסמך היא העלאת סוגיות מהותיות לדיון בתהליך קביעת האסטרטגיה, כאשר יתקדם מחדש במלוא הקשב. המסמך עוסק בהיבטים הקשורים לקידום ההגנה הלאומית ושיפור החוסן הלאומי, ויכולת המשק להתמודד עם תקיפות סייבר רחבות שיש להן השפעה על הביטחון, הכלכלה והחברה.

המסמך, שנכתב טרם פרוץ המלחמה, מצביע על סוגיות מפתח בראיית הכותב, ואינו מתיימר ואין מטרתו להקיף את כלל המורכבויות שבגיבוש אסטרטגיית הגנת סייבר לאומית. הוא נועד להצביע על מורכבות הסוגיות הללו ולייצר בסיס להעמקת הדיון בהן. על מנת לקדם את השיח אין בו המלצות חלוטות וחד-משמעיות. הוא גם אינו עוסק ברכיב ההתקפי בסייבר - למשל, הסוגיה של מדיניות הייצוא של יכולות התקיפות - שהינו רכיב יסוד באסטרטגיית סייבר לאומית כוללת.

המסמך מציג את סוגיות המפתח 'מלמעלה למטה': מההקשר האסטרטגי של הגנת הסייבר הלאומית, איום הייחוס אליו נכון לתת מענה, ויעדי הגנת הסייבר הלאומיים, דרך הסדרת מקומו ויחסיו של מערך הגנת הסייבר בתוך המגזר הממשלתי ומול המגזר האזרחי, ועד מספר התייחסויות למאמצים מרכזיים בתחום הגנת הסייבר.

---

אל"מ (מיל") שי שבתאי הוא חוקר בכיר במרכז בס"א, מומחה לביטחון לאומי, תכנון אסטרטגי ותקשורת אסטרטגית. אסטרטג בתחום הגנת הסייבר ויועץ לחברות מובילות בישראל. שי עומד לסיים את הדוקטורט שלו באוניברסיטת בר-אילן.

סוגיה 1 - 'הפאזל': אסטרטגיית הגנת הסייבר כחלק ממכלול המדיניות הלאומית: כיצד ניתן להגדיר אסטרטגיה ומדיניות הגנת סייבר לאומית בהעדרם של מסמכי אסטרטגיה ומדיניות חלוטים ומאושרים הקובעים עקרונות ארוכי טווח בראייה לאומית כוללת, ובתחומים משפיעים על הגנת הסייבר כמו הביטחון הלאומי, ביטחון הפנים, מדיניות החוץ ותפיסת המחשוב הלאומית?

המלצה: רצוי שאסטרטגיית הסייבר הלאומית תתמקד ככל הניתן בליבת היבטי הגנת הסייבר, ותימנע מלקדם 'יעדים לאומיים' שלא הוגדרו במסגרת חשיבה לאומית רחבה, ותוקפו בהחלטות רשמיות.

סוגיית משנה 1א - הסייבר בתורת הביטחון הלאומי: האם נכון ליצור עבור הסייבר עקרונות תורת ביטחון לאומי נוספים לאלו המסורתיים (העברת המלחמה לשטח האויב, הרתעה, התרעה, הגנה, הכרעה) וכפועל יוצא לשנות את תמהיל המענה בתחום?

המלצה: בשלב ראשון נכון לנקוט ביתר זהירות באימוץ עקרונות מתורת הביטחון הלאומי, שאינם מובהקים להגנת סייבר כמו התרעה והגנה; למשל, ולצמצם את החיבור בינה לבין מושגי יסוד כמו הרתעה והכרעה.

סוגיית משנה 1ב - חיבור הגנת הסייבר למדיניות המחשוב הלאומית: מה צריך להיות תמהיל המענה של הגנת הסייבר הלאומית בין תהליכים ופרויקטים שמטרתם לבנות תפיסות, ארכיטקטורות ואמצעים להגנה על טכנולוגיות עתידיות, גם אם הפרויקטים הלאומיים לא יתממשו בסופו של דבר בהתאם לחזון; לבין ליווי של היבטי ושלבי המימוש המעשיים של פרויקטים אלו, למשל, רק משלב ההכנות למכרז?

המלצה: יש לזהות סוגיות ואזורי מפתח במסגרת הפרויקטים הלאומיים, שבהם קיים צורך מהותי וחשיבות רבה לחשיבה ולתהליכי בניית מענה ארוכי טווח ובהם לבצע היערכות לאומית מקדימה.

סוגיה 2 - תיעדוף איום הייחוס: האם איום הייחוס הלאומי בסייבר המהווה בסיס לקביעת מאמצי ההגנה צריך להעלות את מתארי התקיפה הכלכלית של גורמי פשיעת סייבר מתוחכמים לראש התיעדוף? האם נכון לקחת בחשבון איומים מעצמתיים מצד סין ורוסיה כפרנס משמעותי לא פחות ואף יותר מהאיום האיראני?

המלצה: בקביעת איום הייחוס הלאומי להגנת הסייבר נכון יהיה לתת תיעודף נמוך יותר לשיקולים אסטרטגיים רחבים ולהתמקד בזיהוי ובדרוג הגורמים המציבים את פוטנציאל הנזק הגדול בסייבר ליכולות הלאומיות הממשלתיות והאזרחיות.

סוגיה 3 - מיקוד היעדים הלאומיים בתחום הגנת סייבר: כיצד מביאים לידי ביטוי ביעדים הלאומיים בתחום הגנת הסייבר ובעקרונות המימוש שלהם תפיסה המתמקדת במאמצי הגנת הסייבר על חשבון הקשב לקידום מיזמים בתחומי הכלכלה והביטחון הלאומיים באמצעות הסייבר?

המלצה: בהגדרת היעדים הלאומיים בתחום הגנת הסייבר נכון להתייחס לשניות הלא פתורה בין חזון רחב של מובילות לאומית לבין עיסוק בהגנת סייבר ולהעמיד בראשית הצירים את צרכי הגנת הסייבר. רק לאחר מיצוי המענה לצרכים אלו נכון לשקול הפניית משאבים שירותית לסוגיות שאינן בליבת ההגנה. צרכי ליבה אלו יכולים, למשל, להיות בטווח הקצר והבינוני הגירת גורמים לאומיים ועסקיים לענף הלאומי, ובטווח הבינוני והארוך יכולת הקמת סביבות לאומיות ממודרות בתוך משאבים ציבוריים כמו ענף או מחשוב על.

סוגיית משנה 3א - מעגלי ההגנה הלאומיים: האם אסטרטגיית הסייבר הלאומית יכולה להסתפק בטיפול בתשתיות חיוניות ולצד זאת לבניית תו תקן כללי לכל המשק, או שעליה להעמיק בפילוח כלל המעגלים (תאגידי בין-לאומיים, תשתיות לאומיות קריטיות, ספקי טכנולוגיות מידע ישראלים מרכזיים, גופים גדולים ומפוקחים, חברות בינוניות, עסקים קטנים והציבור הכללי) ולתפור מענה - כולל תשומות לאומיות בעיקר מול התאגידי הבין-לאומיים - ובמענה לכל אחד מהם?

המלצה: במסגרת התהליך האסטרטגי נכון יהיה למפות את המעגלים שלהם הגופים הממשלתיים והעסקיים מתקשים במתן מענה הגנתי עצמאי ושלפעילות המדינה יכולה להיות תרומה משמעותית בסגירת הפערים ולתעדף את המענה לפתרון.

סוגיה 4 - הגישה הבסיסית של מערך הגנת הסייבר: מה הוא התמהיל המיטבי של המודלים האפשריים של ארגונים ממשלתיים (ביטחוני-מבצעי, אכיפת חוק, אסדרה ממשלתית, אסדרה לאומית, גוף אכוונה ומיד) שהמערך יכול לאמץ לעצמו באופן שיאפשר לו למלא את תפקידיו בצורה מיטבית ברמות השונות - ההגנה, המוכנות לאירוע, ניהול האירוע ופעולות האכיפה והתגובה נגד מבצעי האירוע -

ואל מול כלל המעגלים שתוארו בהתאם לחשיבותם? ובנוסף: בהסתכלות ארוכת טווח, האם כדי לקדם שילוב של מערך הגנת הסייבר במשרד ממשלתי שיקצה לו קשב, ממשקים ולעיתים משאבים, שהוא אינו יכול לקבל ממקומו העצמאי כמערך תחת ראש הממשלה?

המלצה: בהחלטות על התמהיל המיטבי של מאפייני מערך הסייבר הלאומי וכפיפותו נכון לקחת בחשבון את שיטות ההשפעה האפקטיביות ביותר של גופים ממשלתיים על הנעשה במשרדי ממשלה ובמגזר העסקי. נכון שמערך הסייבר הלאומי ויחידות הגנת הסייבר במשרדי הממשלה יתמקדו בהגנה על גופים אלו, ולא יעסקו בהיבטים ביטחוניים, מבצעיים ואכיפתיים המטופלים על-ידי ארגונים אחרים. במסגרת זו, על פניו, נראה כי השילוב בין אסדרה, רגולציה ואכיפה שלהם הוא האפקטיבי ביותר.

סוגיה 4 - במגזר הממשלתי: כיצד ניתן לקדם את היבטי הגנת הסייבר במשרדי ממשלה נוספים מעבר לאלו שכבר ביצעו את קפיצת המדרגה (משרד האנרגיה והתשתיות, משרד התקשורת ועוד), ושהגנת הסייבר בהם צריכה לזכות לקשב ולמשאבים מעבר לאלו הניתנים כיום (משרד הבריאות, משרד התחבורה, משרד הפנים, משרד החינוך ועוד)?

המלצה: הגברת המעורבות של מערך הגנת הסייבר ודחיפת פעילות ההגנה בכל משרדי וארגוני הממשלה - ובהמשך להסדרה ברורה של ייעודו ותפקידיו בתחום ההגנה - צריכה להיות יעד מרכזי באסטרטגיה.

סוגיה 4 - מול המשק האזרחי: כיצד יכולה אסטרטגיית הגנת הסייבר הלאומית להביא לתהליכי שיתוף הפעולה המיטביים עם המשק האזרחי, בין היתר, על-ידי מימוש התהליכים המתוארים להלן (טיפול לאומי ב'שרשרת האספקה', רגולציה מקדמת שינוי חיובי, 'שמיכת הגנה', טיפול במחסור בכוח האדם, עבודה עם חברות שירותי הגנת הסייבר) ונוספים?

המלצה: נכון שפתרון המצוקות הרחוביות - בדגש על המחסור בכוח אדם מיומן לתחום הגנת הסייבר - יהיה מנוע מרכזי במערכת היחסים בין מערכת הסייבר הלאומי לבין המשק האזרחי.



סוגיה 5 - מאמצים בתחום הגנת הסייבר הלאומית: עד כמה ובאיזה צורה צריך מערך הסייבר הלאומי וגורמים לאומיים לעסוק במאמצי הגנת הסייבר השונים?

המלצה: בראיית הכותב יש להרחיב מאוד את העיסוק בהכשרת כוח אדם מיומן להגנת הסייבר עבור משרדי הממשלה והמשק האזרחי ולהגמיש את האסדרה בתחום זה; לעומת זאת ניתן לתחם ולצמצם את מאמצי העידוד הלאומיים בתחום מחקר ופיתוח לתחום הגנת הסייבר; נכון למקד ולתחם את המאמץ לקידום שיתופי הפעולה הבין-לאומיים בתחום הגנת הסייבר על-פי סדרי עדיפויות קשיחים יותר תוך גמישות מסוימת להזדמנויות, כולל סיוע חירום למדינות מותקפות; את הלמידה והאימוץ של נורמות חיצוניות להגנת הסייבר נכון לסייג ולהתאים למאפיינים הייחודיים של ישראל; וחשוב לבצע עבודה מטה לאומית לאסדרת פיצוי מס רכוש על אירועי סייבר מצד גורמי תקיפה לאומיים וארגוני טרור.

המסמך נכתב, כאמור, טרם פרוץ המלחמה, ופרסומו התעכב. במסגרת ההתמודדות עם איומי הסייבר במהלך המלחמה ניכרים מאמצים לאומיים מוצלחים מאוד בשילוב בין הגופים הלאומיים - בדגש על מערך הגנת הסייבר - לבין האקוסיסטם האזרחי המרשים הקיים בישראל בתחום ההגנה. מאמצי הגנת הסייבר במהלך המלחמה מחדדים, לדעת הכותב, את הדיון בהקשר של אסטרטגיית הביטחון הלאומי ותורת הביטחון הלאומי, שקרסה באופן כללי ב-7 באוקטובר. הם מצביעים על כיוונים במיקוד יעדי הגנת הסייבר הלאומיים ובהגדרת מעגלי ההגנה הלאומיים, והם מוסיפים נדבכים חדשים והתנסויות בדיון על מקום מערך הגנת הסייבר במגזר הממשלתי ומול המשק האזרחי. מנגד, איום הייחוס שמתממש בשבועות האחרונים תואם תקופת מלחמה, ואינו בהכרח התמהיל הנדרש בהסתכלות על השגרה, שהיא לשמחתנו ממושכת יותר.

ברצוני להודות לרם לוי, מנכ"ל, ודבורה האוסן-כוריאל, יועצת משפטית, של חברת Konfidas; ליאור קלב, ראש תחום הגנת הסייבר ב-Deloitte ישראל; גיא חלפון, מנכ"ל חברת Rescana; ודלית כספי שכנר, מובילת האסטרטגיה באבטחת מערכות מידע של בנק הפועלים על הערותיהם החכמות על הנייר. תכני הנייר הם באחריות הכותב בלבד.

## הקדמה

מטרת המסמך להעלות מספר סוגיות מהותיות לדיון במסגרת הישורת האחרונה של תהליך סיכום אסטרטגיית הסייבר הלאומית בחודשים הקרובים. המסמך מצביע על סוגיות מפתח בראיית הכותב, ואינו מתיימר ואין מטרתו להקיף את כלל המורכבויות שבגיבוש אסטרטגיית הגנת סייבר לאומית. הוא בנוי כך שהוא מציג את סוגיות המפתח הללו 'מלמעלה למטה' - מרמת האסטרטגיה הלאומית ועד למאמצי הגנת הסייבר:

1. סוגיה 1 עוסקת בהקשר האסטרטגי של ההגנת הסייבר הלאומית, וכיצד עליה להתחבר לאסטרטגיה הלאומית; לאסטרטגיה, המדיניות והתורה של הביטחון הלאומי; ולמדיניות המחשוב הלאומית.
2. סוגיה 2 מתייחסת לאיום הייחוס אליו נכון שאסטרטגיית הגנת הסייבר הלאומי תכוון את המענה.
3. סוגיה 3 מצביעה על מרחב הדיון, על יעדי האסטרטגיה ועל החיבור בינם לבין מעגלי הגנת הסייבר המתוארים או רמות הגנת הסייבר הלאומית.
4. סוגיה 4 מנתחת את מורכבות הסדרת מקומו ויחסיו של מערך הגנת הסייבר בתוך המגזר הממשלתי ומול המגזר האזרחי-עסקי כנגזרת של התפיסה האסטרטגית.
5. סוגיה 5 מעלה מספר מאמצים מרכזיים בתחום הגנת הסייבר, ומנתחת היבטים במענה להן.

**סוגיה 1 - 'הפאזל': אסטרטגיית הגנת הסייבר כחלק ממכלול המדיניות הלאומית**  
אסטרטגיה ומדיניות הגנת הסייבר הלאומית אינה עומדת בפני עצמה. למעשה, היא מהווה את הרובד הרביעי של האסטרטגיה והמדיניות הלאומית, וניתן לתאר את מיקומה במדרג כך:



הרובד הראשון הנו האסטרטגיה הלאומית, שבמסגרתה קובעת הממשלה את היעדים הלאומיים בתחומי העל בראייה מצרפית בדגש על מדינית-ביטחונית, כלכלית-חברתית ותשתיתית. לישראל אין אסטרטגיה לאומית כתובה ומאושרת באופן פורמלי. מעת לעת נעשות עבודות יסוד בתחומי ליבה שונים, ואלו אף מיושמות באופן חלקי. היו מספר ניסיונות במוסדות מחקר ליצור מסמך אב כולל, אך הפעולה הלאומית הכוללת אינה מבוססת על אסטרטגיה קוהרנטית. התקדמות משמעותית בהקשר זה בשנים האחרונים היא הפצה, לאחרונה ביולי 2023, של עיקרי תוכניות העבודה השנתיות של משרדי הממשלה ויחידות הסמך, שנותנת לכל הפחות מיפוי טוב של היעדים אותם פועלים לקדם בהעדרה של אסטרטגיה לאומית.

הרובד השני הנו האסטרטגיה בתחום הביטחון הלאומי ובתחום הכלכלי-חברתי. אסטרטגיית הביטחון הלאומי היא מסמך היסוד של הדרג המדיני הנבחר. היא מנתחת את נתוני היסוד ואת ההקשר הרחב של הקיום הלאומי-גאו-פוליטי, כלכלי, דמוגרפי, חברתי, היסטורי, תרבותי, מדיני וביטחוני-צבאי. לאחר מכן מגדירה - על בסיס תפישת העולם של הדרג המדיני - את היעדים הלאומיים (Ends); את היכולות הלאומיות הנדרשות (Means); ואת דרכי הפעולה העקרוניות (Ways) - אלו המאפשרות ליכולות הלאומיות לממש את היעדים הלאומיים. במדינות רבות בעולם מקובל, לעיתים על-פי חוק, שהממשל הנכנס מפרסם National Security Strategy או National Security White Paper. בישראל לא קיים מסמך

כזה. יתר על-כן, בישראל השתרש המונח 'תפישת הביטחון', שעניינו דיון חלקי בכל אחת מרמות הביטחון הלאומי: אסטרטגיה, תורה ומדיניות. כפועל יוצא לא התקיים או מתקיים דיון סדור ורשמי באסטרטגיית הביטחון הלאומי, וגם ניסיון לעגן בחקיקה סמכויות של המטה לביטחון לאומי בתחום זה לא הובילו לשינוי מהותי בתמונת המצב.

במישור האסטרטגיה הלאומית-כלכלית מאז 2006 קיים גוף פורמלי - המועצה הלאומית לכלכלה, שתפקידו "גיבוש והובלת תהליכים אסטרטגיים לקידום המשק והחברה הישראלית". הוא עוסק רבות ברכיבי אסטרטגיה לאומית, ובונה הערכת מצב אסטרטגית כלכלית-חברתית, אך זו אינה מגולמת למסמך אסטרטגיה לאומית בסופו של תהליך.

הרובד השלישי הוא מסמכי התורה והמדיניות:

תורת (דוקטרינת) הביטחון הלאומי, המוכרת במדינות אחרות בעולם כ-National Security Doctrine או National Security Guidance, היא מסמך היסוד של המערכת הביטחונית, ובמהותה אינה מושפעת באופן מידי מתפישת העולם של הדרג המדיני הנבחר. היא מגדירה את מוסכמות היסוד - עקרונות ומושגים - של דרכי ההתמודדות העקרוניות עם אתגרים ביטחוניים-צבאיים. לישראל תורת ביטחון לאומי מוסכמת אך לא פורמלית, ואפרט על הקשר הסייבר שלה להלן.

מהשילוב בין אסטרטגיית הביטחון לבין תורת הביטחון נבנית מדיניות הביטחון הלאומי, המוכרת במדינות אחרות בעולם כ-National Security Policy או National Security Review, שהיא מסמך עקרונות הפעולה של המערכת המדינית-ביטחונית המבטא הערכת המצב הלאומית העיתית ואת הנחיותיו הנוכחיות של הדרג המדיני בסוגיות שעל הפרק. גם מסמך זה לא קיים בישראל, אך אפשר להתייחס להערכת המצב הלאומית השנתית של המועצה לביטחון לאומי (המל"ל) ככזה.

1. מדיניות החוץ היא שם כולל למקבץ היעדים המגדירים את האופן שבו תנהג המדינה ביחס לשאר מדינות העולם. לישראל אין מסמך הפורט את מדיניות החוץ כנגזרת של אסטרטגיית הביטחון הלאומי ומדיניות הביטחון הלאומי. עם זאת, ניתן להתייחס לפרק של משרד החוץ במסמך עיקרי תוכניות העבודה

כסוג של מסמך מדיניות חוץ, על אף שפעילות יחסי חוץ מנוהלת על-ידי משרדי ממשלה וארגונים ממלכתיים אחרים (המוסד, צה"ל), ואינה משוקללת לתוך מסמך זה.

2. מדיניות ביטחון הפנים אמורה להוות גם היא מסמך יסוד להגדרת עקרונות הפעולה של הממשלה בשמירה על ביטחון הציבור, סדרי הממשל התקינים והחוק והסדר. גם כאן ניתן להתייחס במידה מסוימת לפרק של המשרד לביטחון לאומי במסמך עיקרי תוכניות העבודה, כסוג של מסמך מדיניות ביטחון פנים, על אף שאינו מכסה את כלל מאמצי ביטחון הפנים של הממשלה.

3. מדיניות המחשוב הלאומית היא ההסתכלות הכוללת של המדינה על אופן הפיתוח, השילוב והמיצוי של יכולות מחשוב לקידום תשתיות ויכולות פעולה מתקדמות. בתחום זה ביצעה ישראל בשני העשורים האחרונים קפיצות מדרגה, ובמהלך השנה הקרובה מתכוון מערך הדיגיטל הלאומי לגבש "אסטרטגיה מקיפה בכל תחומי פעילות המערך, החל מעיצוב אסטרטגיה דיגיטלית לאומית עדכנית ובהמשך אסטרטגיה בעולמות מערכות המידע הממשלתיות, הדאטה והבינה המלאכותית במגזר הציבורי, אסטרטגיית מעבר הממשלה לענן, אסטרטגיית סייבר ממשלתית ואסטרטגיית שירות מתקדמת". לכך ניתן להוסיף את יעדי משרד החדשנות, המדע והטכנולוגיה בתחומי טכנולוגיות בינה מלאכותית וקוואנטום. על כך בהרחבה להלן.

אלו שלוש הרמות של האסטרטגיה והמדיניות הלאומית שאמורים להיות מבוטאים במסמכים חלוטים ומאושרים - הנמצאים מעל אסטרטגיית ומדיניות הגנת הסייבר הלאומית. 'מלמטה', אסטרטגיה ומדיניות אלו נבנות על בסיס הערכת מצב באשר להשתנות הטכנולוגית ואיום הייחוס, שעליו יורחב להלן.

על-פי תמונת המצב שתוארה, אסטרטגיה ומדיניות הגנת הסייבר הלאומית יכולות להסתמך על מסמכי היסוד הלאומיים באופן חלקי בלבד. לצד החיוב, אמורה להיכתב בתקופה הקרובה אסטרטגיית דיגיטל לאומית, שהיא רכיב קריטי בקביעת עקרונות ההגנה בסייבר, מסמך עיקרי תוכניות העבודה הממשלתיות יכול לסיים עוגן מסוים וכמוהו גם רכיבי תורת הביטחון הבלתי פורמליים והערכת המצב הלאומית של המועצה לביטחון לאומי, שיכולה להיחשב כמדיניות ביטחון לאומי.

נכון וחשוב שמערך הגנת הסייבר יתבסס על מסמכים אלו בבואו לקבוע את האסטרטגיה ואת המדיניות. קביעתן שלא על בסיס עוגנים אלו עלולה להוביל לקביעת יעדים ועקרונות, שאינם בהכרח מחוברים לצורך הלאומי וראה הדיון להלן על מיקוד היעדים הלאומיים.

לצד השלילה, נדבכים מהותיים שאמורים להוות את הבסיס לאסטרטגיה ומדיניות הגנת הסייבר הלאומית חסרים. הדבר בולט במיוחד בראייה ארוכת הטווח, כפי שיפורט להלן. במצב זה ניתן, אולי, לבסס הנחות עבודה סבירות בעיקר בראייה ארוכת טווח, אך לקחת בחשבון שעל אלו להיבחן מחדש לעיתים תכופות - לפחות פעם בשנה ובהינתן התפתחויות בקביעות יסוד לאומיות.

הסוגיה לדיון: כיצד ניתן להגדיר ולמצב אסטרטגיה ומדיניות הגנת סייבר לאומית בהעדרם של מסמכי אסטרטגיה ומדיניות חלטים ומאשרים הקובעים עקרונות ארוכי טווח בראייה לאומית כוללת ובתחומים משפיעים כמו הביטחון הלאומי, ביטחון הפנים, מדיניות החוץ ותפיסת המחשוב הלאומית?

המלצה: מאמצים לאומיים בתחום הסייבר, שאינם מחוברים לאסטרטגיה לאומית כוללת, טומנים בחובם בעייתיות הנובעת מפוטנציאל יצירתן של הטיות באופן בניית האקו-סיסטם של הסייבר כחלק מהמכלול הלאומי. כך, למשל, אפשר לטעון שקיים מיקוד יתר בתעשיית הסייבר הישראלית, באופן שמקשה על קידום מגזרים שעשויים להיות קריטיים לאסטרטגיה הלאומית. לכן, רצוי שאסטרטגיית הסייבר הלאומית תתמקד ככל הניתן - וראה להלן בהתייחסות ליעדי הגנת הסייבר הלאומיים - בליבת היבטי הגנת הסייבר, ותימנע מלקדם 'יעדים לאומיים' שלא הוגדרו במסגרת חשיבה לאומית ותוקפו בהחלטות רשמיות. יצוין, כי דיון בשאלה זו יכול להיות רלבנטי גם למאמצים לאומיים אחרים.

### **סוגיית משנה 1א - הסייבר בתורת הביטחון הלאומי**

כפי שתואר להלן, לישראל תורת ביטחון לאומי מוסכמת אך לא פורמלית. היא עוצבה על-ידי דוד בן גוריון, ונותנת מענה לנחיתות המהותית - בשטח, באוכלוסייה, במשאבים - בין ישראל לבין שכנותיה העוינות באותה התקופה. במוקד עומד הקושי הלאומי להעמיד לאורך זמן כוח צבאי שווה ערך בעוצמתו לזה של מדינות ערב. לכן, בבסיס התורה עומד הרצון לדחות ככל הניתן עימותים צבאיים, ורק בהינתן הצורך, לרכז את מלוא היכולות על מנת להביא להכרעה מול איום צבאי

מדינתי משמעותי המאיים לפלוש לשטח ישראל. יעד זה התבטא בתורת הביטחון המקורית - המוכוונת כאמור לאיום צבאי קונבנציונלי - בשלושה עקרונות מרכזיים: אסטרטגיה מגננתית ופעולה התקפית, 'צבא העם' ו'משולש הביטחון'.

אסטרטגיה מגננתית ופעולה התקפית: בן גוריון גיבש עקרון יסוד, לפיו האסטרטגיה הצבאית הישראלית היא מגננתית, קרי - תגובתית לאיומים כחלק מהרצון לשמר תמיכה בין-לאומית ושואפת לפעול בקווים הפנימיים. עם זאת היא באה לידי ביטוי בפעולה התקפית המעתיקה מוקדם ככל הניתן את המלחמה לשטח היריב על מנת ששדה הקרב העיקרי לא יהיה בשטח המדינה הקטן.

'צבא העם': זה"ל התבסס על גיוס חובה, שאפשר לו לקיים כוח סדיר קטן יחסית, שעסק במשימות הביטחון השוטף; הכין את זה"ל למלחמה; ובמידת הצורך אמור היה להגן בשלבים הראשונים של המלחמה. מעבר לגרעין הסדיר ועל בסיסו, בונה צבא מילואים גדול, ששימר מוכנות למלחמה. בהינתן פקודה יכול היה צבא המילואים להתגייס בזמן קצר יחסית ולהפוך את זה"ל לצבא גדול מספיק להתמודדות מול קואליציה צבאית.

'משולש הביטחון': הצורך לדחות ככל הניתן את העימותים, ובהינתן התפתחותם להגיע לסיום מהיר, הוביל לגיבוש שלושה מושגי יסוד. אלו כוונו לאיום צבאי מדינתי, אך עודכנו במעלה הדרך - כולל במסגרת דינוי ועדת מרידור - לתת מענה לסוגי איומים נוספים:

1. הרתעה: ישראל תשמר את הבסיס לעליונות ברורה ביכולות על יריביה הפוטנציאליים, ותשדר נחישות, באופן שיוביל את מקבלי ההחלטות בצד האחר להסס ולדחות החלטה להיכנס עימה לעימות. מושג ההרתעה הורחב במעלה הדרך על מנת לאפשר לו רלבנטיות בתחום המאבק בטרור.
2. התרעה: ישראל תזהה שינויים בכוונות מקבלי ההחלטות של היריב ובמוכנות כוחותיהם הצבאיים באופן המעיד על הכנות לעימות בזמן מספיק לגיוס לקראתו את מלוא עוצמתו של זה"ל - בדגש על צבא המילואים. תחום ההתרעה הורחב בעשורים האחרונים לכל סוגי האיומים האפשריים. הרחבה זו הביאה להגדלה משמעותית של היקף האחריות על קהילת המודיעין.
3. הכרעה: לאור העדר עומק אופרטיבי בשטח מדינת ישראל, ייצא זה"ל מוקדם ככל הניתן - רצוי עם תחילת העימות ואף ביוזמתו ("מלחמת מנע",

"מכת מנע") - למתקפה, שתעביר את הלחימה לשטח האויב. המתקפה תשיג הכרעה מהירה תוך ימים / שבועות ספורים, שמשמעותה פגיעה קשה ביכולות האויב, שתיצור את התנאים לפרק זמן ארוך יחסית של שקט. בעשורים האחרונים מנסים להחיל את מושג ההכרעה להקשרים נוספים - נב"ק, טרור - אך דבר זה הנו מורכב ולעיתים אינו מעשי.

בדיוני וועדת מרידור, שפעלה בין 2003 ל-2006, הוחלט - מעבר להרחבת היריעה של המושגים הקיימים - לצרף מושג יסוד נוסף - רביעי - ל'משולש הביטחון' והוא ה'התגוננות' או בשפה מרחיבה 'הגנה'. עיקרון זה מעגן בתורת הביטחון את המצב בשטח. מדינת ישראל משקיעה חלק ניכר מתקציב וממאמצי הביטחון שלה על התגוננות פאסיבית. לאלו ניתן לצרף מערך אבטחה - ציבורי ופרטי - רחב ממדים. מרחיבי הרעיון להגנה מוסיפים לכלי ההתגוננות הפאסיביים כלים התקפיים נקודתיים שמטרתם סיכול ירי תלול מסלול או פיגועי טרור מתחת לרף ההסלמה הרחבה.

סקירה קצרה זו מעלה תהיה, האם תורת הביטחון של ישראל רלבנטית לתחום הסייבר. תנאי היסוד של תחום הסייבר שונים בתכלית מאלו שאפיינו את ביטחון ישראל בשנות החמישים. תווך הסייבר משבש מושגים של גבולות וריבונות העומדים במוקד התורה המקורית, ובמסגרתו לישראל:

1. יתרון טכנולוגי מובהק בתחום הסייבר על פני מדינות המזרח התיכון.
2. יתרון משאבי מובהק בתחומים הטכנולוגי והאנושי על פני מדינות המזרח התיכון בתחום הסייבר.
3. פוטנציאל יכולת ההגנה של ישראל בסייבר מאפשר לה להתמודד עם התקפות משמעותיות ללא צורך 'להעביר את המלחמה לשטח היריב', קרי, לפעול ל'הכרעה' של מערכי הסייבר שלו.
4. ישראל מקיימת שיתוף פעולה ולא יריבות בתחום הסייבר עם מדינות מפתח באזור בדגש על מדינות 'הסכמי אברהם'.

מתנאי היסוד האלו בתחום הסייבר עולה סימן שאלה גדול באשר לרלבנטיות עקרונות תורת הביטחון הקיימים עבורו. פרסומים זרים מייחסים לישראל ביצוע תקיפות תגובה בסייבר באיראן. הרמטכ"ל, רב-אלוף אביב כוכבי, ציין במאי 2020, ברקע הדיווחים על 'מלחמת סייבר' עם איראן לאחר תקיפה המיוחסת לישראל נגד



נמל איראני, כי "נמשיך לפעול בכלים מגוונים". אם אכן ישראל מבצעת תקיפות סייבר באיראן כחלק מהמערכה בתחום הסייבר לצרכי 'הרתעה' ו'הכרעה' של היריב, נשאלת השאלה האם נכון ליישם את רכיבי תורת הביטחון המסורתית של ישראל בתחום זה.

בהפוך על הפוך לגישת היסוד של תורת הביטחון המסורתית, העוצמה הישראלית במרחב הסייבר מאפשרת לישראל, למשל, להתמקד בהתגוננות מול היריב ולסכל את רוב התקפותיו או לכל הפחות להקטין מאוד את השפעותיהן העסקיות והתפעוליות. בכך היא מאפשרת לקיים 'הרתעה במניעה' (Deterrence by Denial) ללא צורך להשקיע משאבים בהתקפות תגובה לצרכי 'הרתעה בענישה' או 'הכרעה'. אפשר שנכון יותר להגיב להתקפות באמצעות מהלכים דיפלומטיים ופוליטיים בין-לאומיים, שיבודדו את איראן, ויגרמו לה לשלם מחירים אסטרטגיים על האגרסיביות שלה בתחום הסייבר מאשר להגיב בפעולה התקפית בסייבר או על סייבר בתווך אחר. לכך מצטרפת העובדה, כפי שתואר להלן בהתייחסות לאיום הייחוס, שהאיומים על ישראל בתחום הסייבר מגיעים מצד שחקנים, שתורת הביטחון אף פחות רלבנטית להם.

הסוגיה לדיון: האם נכון בתחום הסייבר ליצור עקרונות תורת ביטחון לאומי אחרים לאלו המסורתיים וכפועל יוצא לשנות את תמהיל המענה לאיומים?

המלצה: כצעד מקדים למהלך הגדרת עקרונות תורת ביטחון לאומי ייעודיים בתחום הסייבר נכון לנקוט ביתר זהירות באימוץ עקרונות, שאינם מובהקים להגנת סייבר כמו התרעה והגנה. במסגרת זה ניתן לעלות סימני שאלה מהותיים על רלבנטיות מושגי ההרתעה וההכרעה לתחום. יצוין, כי דיון בשאלה זו יכול להיות רלבנטי גם לתחומים אחרים בתחום הביטחון הלאומי.

### סוגית משנה 11 - חיבור הגנת הסייבר למדיניות המחשוב הלאומית

כאמור, מדינת ישראל התקדמה בעשורים האחרונים במידה ניכרת בתחום מדיניות המחשוב הלאומי: בניית הממשל הזמין (egov), הקמת מערך הדיגיטל הלאומי, פרויקט הענן הלאומי (נימבוס), התקדמות ביישומי מידע ובינה מלאכותית במשרדי הממשלה, קידום הפריסה של תשתית תקשורת מתקדמת בשנים האחרונות, העיסוק במחשוב על ובקוואנטום ועוד - כל אלו מעידים על רצון ודחיפה להצעיד את תשתיות המחשוב של ישראל למקום מתקדם ומוביל עולמית.

עם זאת, לאורך השנים החזון והתוכניות השאפתניות נתקלו בקשיי מימוש, צומצמו או שיישומם נפרס על פני שנים רבות. היישום בפועל מתממש אך שונה, לעיתים במהותו, מהתוכניות המקוריות. כך, למשל, ביקורת של מבקר המדינה על שימוש משרדי ממשלה בענן ציבורי והיערכות להקמת ענן מרכזי, קבעה, כי "בשנת 2019 השקיעה הממשלה במחשוב ענן פחות מאחוז אחד מסך השקעתה בתקשוב, לעומת 8% בעולם". באשר לסטטוס פרויקט נימבוס קבע הדו"ח:

"פרויקט נימבוס הוא פרויקט רב-שנתי שהחל בשנת 2019 ושנועד לתת מענה מקיף לנושא אספקת שירותי ענן למשרדי הממשלה. הפרויקט מורכב מארבעה רבדים המרכיבים את המרכז המרכזי של מינהל הרכש הממשלתי. במהלך שנת 2020 פורסמו מכרזים לרובד הראשון (אספקת שירותי ענן) והרובד השני (מרכז מצוינות במחשוב ענן) של המרכז, ובמהלך פברואר 2021 פורסם מכרז לרובד השלישי (שירותי מודרניזציה והגירה). טרם פורסם מכרז לרובד הרביעי (שירותי ניטור ומיטוב), ולא נקבע מועד משוער לפרסומו. אי-קיומה של מסגרת זמנים מוגדרת לפרויקט בכללותו עלולה להביא להתארכות יישומו ולעיכוב בתוכנית להעברת משרדי הממשלה לסביבת הענן".

באשר להיבטי הגנת הסייבר של השימוש בענן ציין הדו"ח, כי:

"על אף הנחיה ייעודית של מנהל היחידה להגנת הסייבר בממשלה (להלן - יה"ב) הקובעת כי כל מערכת אשר פועלת בסביבת הענן נדרשת לאישור הוועדה המייעצת לנושא העברת מידע ויישומי מחשוב לסביבת הענן הציבורי... מתשובותיהם של 42 משרדים על השאלון שהפיץ משרד מבקר המדינה עולה כי במשרדים אלה פועלות בלא שהתבקש אישור הוועדה המייעצת כעשר מערכות בסביבת ענן. הפעלת מערכות כאמור בסביבת ענן בלא שהוועדה בחנה אם יש מקום לאשרן עלולה להביא להתממשות סיכוני אבטחת מידע הכרוכים בהפעלת מערכות אלה".

גם בתחום מחשוב העל החיוני, בין היתר, לקידום התוכנית הלאומית לבינה מלאכותית, דווח, כי פרויקט מחשב העל הלאומי מ-2020 פוצל לשלושה פרויקטים מצומצמים יותר: שימוש במחשבי על באמצעות שירותי הענן של ספקיות בין-לאומיות גדולות במסגרת פרויקט נימבוס, השתתפות בפרויקט רשת מחשבי

העל של האיחוד האירופי במסגרת מיזם 'אירופה דיגיטלית' והקמת מעבדת מחשב על ובינה מלאכותית. אחת ההצעות שהוגשו במסגרת פרויקט זה הנה של אנבידיה (Nvidia), יצרנית שרתי הבינה המלאכותית (AI) הגדולה בעולם, אך זו לא מחכה לפרויקט הלאומי, וכבר השיקה באמצע 2023 את מחשב העל הישראלי שלה Israel-1, אך הצהירה כי הוא ישמש אותה למחקר ולפיתוח ובהמשך למתן שירותים למגזר הפרטי.

בתחום הקוואנטום קיימת הצהרת כוונות בדמות עיצובה של תוכנית לאומית מרכזית, אך נראה כי תהליך ההתקדמות בתחום זה עדיין מבוזרת, מבוססת על יוזמות של מוסדות אקדמיים והתארגנויות עסקיות, ואינה רחבה ועמוקה מספיק יחסית לגודל האתגר.

מצב זה, שבו קיימים רכיבי מפתח במדיניות מחשוב לאומית אך אלו מיושמים באופן חלקי ומתמשך הרבה יותר מהמתוכנן, יוצרת דילמה עבור הגנת הסייבר הלאומית. מצד אחד פרויקטים בסדר גודל כזה יש ללוות בהיבטי הגנה משלב הבחינה וטרם הפרויקט. על מנת לבנות ארכיטקטורת הגנה לתשתיות מחשוב כה נרחבות ומתקדמות, שעבור חלק מהיבטי ההגנה שלהן אף לא קיימות כיום בשוק טכנולוגיות הגנה רלבנטיות, נדרש תהליך מתמשך ויקר של למידה, התייעצות ואף התבססות על מומחים חיצוניים, תכנון ויישום בזמן של היבטי ההגנה. הגנת הסייבר של פרויקטים לאומיים גדולים כבר נפגעה בעבר מאי-קיומו של תהליך כזה. מהצד האחר, רידוד והתמשכות היישום של הפרויקטים והצורך להתאים את חליפת ההגנה 'בתנועה' לארכיטקטורות מעודכנות משמעותן השקעה - לעיתים ניכרת - של משאבים נוספים.

הסוגיה לדיון: בחיבור הגנת הסייבר למדיניות המחשוב הלאומית, מה צריך להיות תמהיל המענה של הגנת הסייבר הלאומית בין תהליכים ופרויקטים שמטרתם לבנות תפיסות, ארכיטקטורות ואמצעים להגנה על טכנולוגיות עתידיות, גם אם הפרויקטים הלאומיים לא יתממשו בסופו של דבר בהתאם לחזון; לבין ליווי של היבטי ושלבי המימוש המעשיים של פרויקטים אלו, למשל, רק משלב ההכנות למכרז?

המלצה: יש לזהות סוגיות ואזורי מפתח במסגרת הפרויקטים הלאומיים, שבהם קיים צורך מהותי וחשיבות רבה לחשיבה ולתהליכי בניית מענה ארוכי טווח, ובהם לבצע היערכות לאומית מקדימה. צרכי ליבה אלו יכולים, למשל, להיות בטווח

הקצר והבינוני הגירת גורמים לאומיים ועסקיים לענן הלאומי, ובטווח הבינוני והארוך יכולת הקמת סביבות לאומיות ממודרות בתוך משאבים ציבוריים כמו ענן או מחשוב על.

## סוגיה 2 - תיעדוף איום הייחוס

הקדמה מתודולוגית קצרה: איום הייחוס אינו תיאור של סך האיומים האפשריים - במקרה זה בתחום הסייבר - על מדינת ישראל - מעין 'תמונת מודיעין' של סך האיומים האפשריים. הוא גם אינו ניתוח של מכלול הסיכונים הקיימים. איום ייחוס הוא סוג של 'ניתוח-על' - היער ולא העצים - שמטרתו לאפשר לגורמים הקובעים לקבל החלטות מושכלות לגבי אסטרטגיית הגנת הסייבר הלאומית.

איום הייחוס מגדיר - על בסיס האסטרטגיה הלאומית - מה הם היעדים והנכסים המרכזיים, שפגיעה בהם על-ידי גורם עוין תחליש את המדינה. הוא מתחיל בלשאול שאלה על עצמנו - מה חשוב לנו?

לאחר מכן הוא בוחן את סוגי היריבים האפשריים, היכולות שלהם והיעדים שלהם. הוא ממפה אירועים עקרוניים ומשמעותיים (ולא סך 'הדברים הרעים') שיכולים לקרות. הוא בודק מה רמת ההגנה של המדינה בשלב הנוכחי - קרי, איזה אמצעי ותהליכי הגנה מיושמים או אמורים להבשיל בתקופה הקרובה, ומה רמת ההגנה שהם מספקים. אם לא היינו משקללים את רמת ההגנה הקיימת, האיום היה מוחלט (בשפת ניהול הסיכונים - התממשות 'הסיכון השורשי'): כל 'לד' היה יכול להפסיק את החשמל במדינת ישראל, כי שום דבר לא היה עומד בדרכו, וזה כמובן לא המצב.

התוצאה היא תיאור של 'הדברים הגדולים': מתארי האיום בעלי המשמעות שיכולים לקרות למדינה בתחום הסייבר. התיאור הזה מאפשר למקבלי ההחלטות הבכירים להחליט בפני מה חשוב להגן, מה סדר העדיפויות, כמה משאבים חשוב להשקיע, ובאילו מאמצי הגנה חשוב להתמקד. אם לא פועלים בצורה כזו, קשה למקבל ההחלטות הלאומי להבין את איום הסייבר. ירידה רבה מדי לפרטים טכניים יוצרת ריחוק בין מקבל ההחלטות - שגם כך הסייבר קשה לו לעיכול - לבין הגורמים המקצועיים המצויים לעומק בפרטים.

תמונת האיום הנוכחית מעלה דילמה משמעותית. בכתבה בהארץ (12 ביולי 2023) הגדיר ראש מערך הסייבר הלאומי, גבי פורטנוי, את איראן כאיום העיקרי.

לדבריו, עיקר המתקפות מגיעות מאיראן, שבה פועלות בשנה האחרונה 15 קבוצות האקרים, לעומת חמש בשנה שלפניה, המתקפה הקשה ביותר הייתה על הטכניון, אך נראה שלא הוצא מידע משמעותי. איראן גם מסייעת לחיזבאללה ולחמאס לשדרג את יכולות ההגנה והתקיפה בסייבר. לדברי הכתב סירב ראש מערך הסייבר להתייחס למדינות נוספות שתוקפות את ישראל בעיקר למטרות של איסוף מידע, ופחות לגרימת נזקים למוסדות ולגופים, ובהן סין ורוסיה.

עם כן, מדינת ישראל מדרגת את האיום מצד איראן ושותפיה כמתאר החמור ביותר, ומזהה תקיפות למטרות איסוף מידע רגיש של המעצמות. מדובר בהסתכלות ביטחונית במאפייניה על איום הסייבר הלאומי, שמכוונת בראש ובראשונה למדינות או ישויות אויבות, לאחר מכן לפוטנציאל האיום מצד מעצמות ותוך פחות דגש על איומי סייבר אזרחיים. נראה כי התיעודף הזה משפיע גם על המענה הישראלי, כפי שבא לידי ביטוי, כאמור, על-פי פרסומים זרים וייחוס של אירועי סייבר בתקיפות תגובה המיוחסות לישראל באיראן.

האם אלו הם האיומים המשמעותיים ביותר?

עיקר איום הסייבר על מדינות מתקדמות הוא מצד גורמי פשיעה מתקדמים במסגרת מתקפות כופר וסחיטה. הפגיעות המשמעותיות ביותר בשנים האחרונות - במיוחד מאז הקורונה - הנן השבתה של ארגונים אזרחיים גדולים במתקפות כאלו. אלו גרמו לפגיעה בתשתיות קריטיות דוגמת אספקת הגז בחוף המזרחי בארצות הברית (קולוניאל פייפליין, מאי 2021), מוסדות רפואיים משמעותיים (בית חולים CHSF ליד פריז, אוגוסט 2022) ופגיעה ברמה הלאומית (ממשלת קוסטה ריקה, אפריל 2022). מאחורי חלק מהפעולות של חברות פשיעה אלו עומדת גם דחיפה של מניעים לאומיים, אך מהות התקיפות היא אופורטוניסטית לחלוטין, וייתקפו ארגונים על בסיס נגישות טכנולוגית ורמת המסוגלות העסקית.

הסוגיה לדיון: האם איום הייחוס בסייבר הלאומי המהווה בסיס לקביעת מאמצי ההגנה צריך לתעדף את מתארי התקיפה הכלכלית של גורמי פשיעת סייבר מתוחכמים? האם נכון לקחת בחשבון איומים מעצמתיים מצד סין ורוסיה כפרנס משמעותי לא פחות ואף יותר מהאיום האיראני?

ברי כי להרכב שונה של איום הייחוס תהיה השפעה על החלטות של תמהיל המענה לאיומים: היכן ממקדים את איסוף המודיעין הלאומי? כיצד מטפחים

מודיעין סייבר מסחרי רלבנטי לתמהיל האיום? מה חלוקת הקשב של מאמצי ההגנה, הניטור וההתרעה? מול אלו איומים ממקדים את המענה הלאומי בתחום ההגנה האקטיבית (תקיפות סייבר לצרכי מניעה), הסיכול וההרתעה?

המלצה: בקביעת איום הייחוס הלאומי להגנת הסייבר נכון יהיה לתת תיעודף נמוך יותר לשיקולים אסטרטגיים רחבים - למשל, מי הם גורמי האיום בממדים אחרים על מדינת ישראל - ולהתמקד בזיהוי ובדרוג הגורמים המציבים את פוטנציאל הנזק הגדול בסייבר ליכולות הלאומיות הממשלתיות והאזרחיות.

### סוגיה 3 - מיקוד היעדים הלאומיים בתחום הגנת סייבר

מסמך אסטרטגיית הגנת הסייבר הקיים מ-2017 קבע את חזון הסייבר של מדינת ישראל: "מדינת ישראל תהיה מדינה מובילה ברתימת מרחב הסייבר לטובת צמיחתה הכלכלית, רווחתה החברתית וביטחונה הלאומי". ניסוח זה מבוסס על המלצות המיזם הקיברנטי מ-2011. חזון הסייבר הנוכחי - עד לשינויו - של מדינת ישראל אינו כולל בצורה מפורשת הגנה לאומית בסייבר.

תפיסת הפעולה למימוש החזון - שניתן אולי להגדירה כיעדי הגנת הסייבר הלאומיים - כוללת שלושה רכיבים:

1. עמידות משקית: "היכולת של ארגונים במשק ושל תהליכים בין-ארגוניים ומשקיים להתמיד בפעילות תחת שגרת איומי סייבר". רכיב זה מקודם באמצעות אסדרה ישירה ועקיפה של ארגונים במשק ותהליכי אסדרה בשוק הגנת הסייבר.

2. חוסן מערכתי: "יכולת ההתמודדות של המדינה והארגונים בה עם תקיפות סייבר באופן שיטתי, לשם צמצום הנזק המצטבר במשק לקראת אירוע, במהלכו ולאחריו". רכיב זה מקודם על-ידי תהליכים מדינתיים של שיתוף מידע וסיוע לארגונים שנתקפו.

3. הגנה לאומית: "ניהול מערכה מדינתית נגד איומים חמורים, אשר עומדים מאחוריהם תוקפים נחושים ובעלי משאבים, המהווים סיכון ממשי לביטחון המדינה".

יעדי הגנת הסייבר הלאומיים - בשונה מהחזון - ממוקדים בהגנת סייבר: בניית יכולת הגנה למניעה, התמודדות עם אירועי סייבר כאשר מתרחשים, וניהול מאמצים כוללים להחלשת איומים בתחום הסייבר.

למימוש יעדים אלו מוגדרים חמישה מאמצים - שלושת הראשונים הם מאמצי על, והשניים הנוספים תומכים:

1. בניית הסייבר כמרחב צמיחה בטוח: מאמץ כלל-ממשלתי הכולל חיזוק ההגנה בארגונים במשק, קביעת אמת מידה גבוהה בהגנה על גופי הממשלה, ומאמצים ליישום פתרונות, תהליכים ותשתיות ברמה הלאומית.
2. הקמת הרשות הלאומית להגנת הסייבר וקידום היערכות לאומית משלימה: גוף מרכזי להגנת סייבר שזהו ייעודו היחיד.
3. מחקר, פיתוח ויישום של יכולות וטכנולוגיות הגנה מדינתיות.
4. בניין הכוח המדעי-טכנולוגי הלאומי בסייבר כיתרון היחסי של מדינת ישראל.
5. שותפות במאמצים בין-לאומיים לעיצוב מרחב הסייבר.

מטרתם של מאמצי הגנת הסייבר הלאומיים רחבה יותר מיעדי ההגנה הלאומיים הממוקדים בהגנה, והם מתכתבים עם החזון של מדינה מובילה בתחום הסייבר. המשמעות היא שבאסטרטגיה הלאומית הקיימת יש שניות לא פתורה בין חזון רחב של מובילות לאומית לבין עיסוק בהגנת סייבר.

ניתן להשוות את יעדי ומאמצי הגנת הסייבר לאסטרטגיית הסייבר הלאומית של ארצות הברית ממרץ 2023. גישת הבסיס של האסטרטגיה היא יצירת "נתיב ל[קיום] חוסן במרחב הסייבר". היא מדגישה שלושה עקרונות: "איון מחדש של האחריות להגנת מרחב הסייבר" בין המשתמשים במרחב לבין חברות הענק המעצבות ויוצרות את האקוסיסטם הדיגיטלי; "בנייה מחדש של התמריצים באופן שייתן תיעודף להשקעות ארוכות טווח"; והתבססות על ההישגים של המדיניות הנוכחית.

על מנת לממש את גישת הבסיס מוגדרים חמישה יסודות, שכל אחד מהם מפורט ליסודות משנה:

1. יסוד אחד: הגנה על תשתיות קריטיות.
2. יסוד שני: שיבוש והשבתת גורמי האיום.
3. יסוד שלישי: עיצוב כוחות שוק שידחפו להגנה ולחוסן.
4. יסוד רביעי: השקעה בעתיד חסין יותר.
5. יסוד חמישי: יצירת שותפויות בין-לאומיות על מנת לחתור להשגת יעדים משותפים.

ניתן לראות מכותרות אלו, והדבר בא עוד יותר לידי ביטוי ביסודות המשנה, שהאסטרטגיה האמריקנית ממוקדת בצמצום החולשות המובנות ובטיפול בפוטנציאל האיום: הגנה מפני איומי הסייבר על-ידי סגירת פרצות בקווי ההגנה ובטכנולוגיות המידע הקיימות; הקטנתן בראייה ארוכת טווח; ופעילות פרו-אקטיבית בשיתוף פעולה בין-לאומי על מנת לרדוף, לשבש ולהשבית את גורמי האיום.

גישה דומה המתמקדת בהגנה ובצמצום האיום ניתן לזהות במטרות תוכנית העבודה של מערך הגנת הסייבר לשנת 2023. ארבעת המטרות הראשונות מתוך שבע הן: הקמת כיפת סייבר לאומית ובתוכה SOC לאומי; מימוש תפיסת הגנה סקטוריאלית ומשקית; הכוונת פעילות ההגנה על-פי מדדים לאומיים; ומתן מענה טכנולוגי להגנת הסייבר המדינתית. שלושת היעדים הבאים מתכתבים עם מיקוד בהגנה: קידום האינטרסים הלאומיים באמצעות שותפים בין-לאומיים; גיבוש אסטרטגיה מדינתית ותפיסה רגולטורית; ושילוב ההזדהות החכמה במערך הגנת הסייבר.

נראה כי הגישה האמריקנית והישראלית הנוכחית מתמקדות בהיבטי ההגנה, ומפחיתות את העיסוק בקידום הגנת הסייבר כמכפיל כלכלי ומדיני לאומי מתוך הבנה שהחולשות הקיימות מחייבות מיקוד בפערי ההגנה וההתמודדות עם אירועי ואיומי הסייבר. זו הסתכלות ריאלית על הקשר הסייבר, ולא כזו שמנסה לחולל - בהעדר מסמכים לאומיים אסטרטגיים כפי שתואר - הקשר לאומי אסטרטגי רחב לסוגיה.

הסוגיה לדיון: מיקוד היעדים הלאומיים בתחום הגנת הסייבר: כיצד מביאים לידי ביטוי ביעדים הלאומיים בתחום הגנת הסייבר ובעקרונות המימוש שלהם תפיסה המתמקדת במאמצי הגנת הסייבר על חשבון הקשב לקידום מיזמים בתחומי הכלכלה והביטחון הלאומיים באמצעות הסייבר?

המלצה: בהגדרת היעדים הלאומיים בתחום הגנת הסייבר נכון להתייחס לשניות הלא פתורה בין חזון רחב של מובילות לאומית לבין עיסוק בהגנת סייבר, ולהעמיד בראשית הצירים את צרכי הגנת הסייבר. רק לאחר מיצוי המענה להם נכון לשקול הפניית משאבים שירית לסוגיה שאינן בליבת ההגנה.



### סוגיית משנה 3א - מעגלי ההגנה הלאומיים

מדינת ישראל בחרה להגן על הגופים המרכזיים במשק מפני איומי סייבר הנובעים משרשרת האספקה שלהם באמצעות רגולציה מגזרית המחייבת לבחון בערוץ חד-כיווני - לקוח-ספק באמצעות שאלונים וסקרים את ההגנה שלהם. בצורה זו, מכלול רחב של ארגונים עסקיים גדולים, בינוניים וקטנים, המספקים לגופים המרכזיים במשק מוצרים ושירותים מהותיים לפעילותם, נדרשים לשפר את התנהלותם בתחום באופן התורם לרמת ההגנה הכוללת של המדינה ושל המשק. לשיטה זו יתרונות מובהקים משום שהיא מבוססת על האמצעים היעילים של ציות לרגולציה ותמריצים עסקיים, והיא ממקדת את המענה לסביבת העבודה של המגזרים המרכזיים במשק.

עם זאת, גישה זו טומנת בחובה מספר בעיות מהותיות. המונח 'שרשרת אספקה' נולד מתוך זווית הראייה של הארגונים הגדולים, שמבחינתם קיימים תהליכים לינאריים, שבמסגרתם הם מרכזים תשומות ממספר רב של מקורות ('הספקים') על מנת לייצר תפוקות אותם הם מוכרים לצרכנים ('הלקוחות').

העולם היום הוא רשתי ולא לינארי. דימוי 'השרשרת' נכון שיפנה את מקומו לתפיסת 'הרשת'. כמעט כל גורמי הערך במשק יכולים למצוא עצמם הן בצד של 'הלקוח' והן בצד של 'הספק'. בעולם כזה הצומת או הקישור החלשים (ולא 'החוליה' כמו בדימוי השרשרת) עשויים להפיל את הרשת כולה (הכוללת גם את הספק של הספק של הספק או את הלקוח שהוא גם ספק וכו'). במדינה קטנה הפונה לעולם, כמו ישראל, הרשת הלאומית היא רק חלק קטן מרשת גלובאלית רחבה. הדבר בולט במיוחד בתחום טכנולוגיות המידע. כך, למשל, באירוע NotPetya ב-2017, הותקפה אוקראינה באמצעות תוכנת ניהול החשבונות פגעה בתפקוד, בין היתר, של ענקית הספנות הדנית Maersk, ענקית המשלוחים האמריקנית FedEx ויצרנית התרופות האמריקנית Merck.

בעיה נוספת בגישת 'שרשרת האספקה' היא ההטיה המובהקת לקידום רמת ההגנה באמצעות שאלונים וסקרים. 'הלקוח', הגדול ורב המשאבים, לא מסייע בפועל ל'ספק' לשפר את רמת המענה שלו להגנת הסייבר, אלא מדרבן אותו באמצעות 'ציונים'.

הפתרון לפערים אלו יכול להגיע ממעבר מגישת 'שרשרת האספקה' לגישה כוללת יותר של 'רשת אספקה', שבמסגרתה הארגונים הממשלתיים והגופים העסקיים הגדולים יחתרו לחזק רשת מוגנת יותר מסביבם, שתתבסס על רגולציה והנחייה אך גם על מהלכים מעשיים לבניית הגנה אפקטיבית בכל המעגלים.

איך בונים רשת כזו? מתייחסים להגנת הסייבר בפועל בכל רכיביה במסגרת תפיסה משולבת ומסונכרנת ברמה הלאומית. במסגרת זו, למשל ניתן לציין את המעגלים הבאים:

1. תאגידים בין-לאומיים: הספקים המשמעותיים ביותר של המשק הישראלי, במיוחד בטכנולוגיות מידע, הינן חברות הענק (למשל: מיקרוסופט ואמזון בענן, סיקו ואינטל בחומרה, סילספורס, סוויפט בהעברות הכספים, רויטרס במסחר הבורסאי ועוד). לצד פעולות הפחתת סיכונים והגנה ארגונית נדרש מהלך בתכלול לאומי מול תאגידים אלו על מנת לחזק ההגנה, בדגש על קניין רוחני ומידע פרטי. לאור גודלם ופריסתם של תאגידים אלו, מהלך אפקטיבי מחייב שיתוף פעולה מולם ותיאום עם ממשלות אחרות. ארצות הברית, למשל, כבר מטילה על תאגידים אלו - במסגרת אסטרטגיית הסייבר הלאומית העדכנית - אחריות גדולה יותר מבעבר על הגנת הסייבר שלהן ושל לקוחותיהן, ואפשר להסתמך על המאמץ האמריקני בתחום. מערך הסייבר כבר מכוון לקשר עם תאגידים בין לאומיים אלו, כפי שמתבטא ביעד 5.2 של תכנית העבודה ל-2023.
2. תשתיות לאומיות קריטיות: בזק, ספקיות האינטרנט והסלולר, חברת חשמל ועוד מהווים סוג נוסף של ספקים משמעותיים. ההגנה שלהם מנוהלת בראייה לאומית לרוב בהנחיית מערך הסייבר הלאומי על-פי חוק, ובשנתיים האחרונות אף בוצעה קפיצת מדרגה בהגנה על ספקיות התקשורת. נדרש להוסיף תיאום בינם לבין יתר המשק ('לקוחותיהם') לגבי שיתוף פעולה במאמצים לאיתור ולטיפול באירועי סייבר במערכות שלהם וליבון המוכנות הנדרשת כתוצאה משיבוש שירותיהם. צעדים משמעותיים בכיוון זה נעשו בשנים האחרונות בשיתוף הפעולה בין משרד התקשורת לבין מערך הסייבר הלאומי, ומניעת תקיפות סייבר המשביתות חברות תקשורת גדולות מוגדר על-ידי המשרד כיעד ל-2023.
3. ספקי טכנולוגיות מידע ישראליים מרכזיים: מספר חברות גדולות (למשל: רד- בינת ומלם-תים, פלטפורמות מסחר כמו FMR וסיברון) מעניקות שירותים

בקנה מידה רחב, וחלקן אף מהוות לעיתים ספקיות בלעדיות בתחומן. בשונה מחלק מלקוחותיהן הן אינן כפופות לרגולציה מחמירה בתחום הגנת הסייבר. נדרשת חשיבה על מענה מנוהל ברמה הלאומית לגופים כאלו.

4. גופים גדולים ומפוקחים: הגופים הגדולים במשק, שחלקם - בעיקר הפיננסיים - נתונים לרגולציה ולפיקוח בתחום הסייבר, צריכים להוות את המחוללים ואת המאיצים של העלאת רמת ההגנה הכוללת. לצורך כך נכון יהיה לשקול להרחיב את רגולציית ההגנה המחייבת, למשל, לכל החברות הכפופות להוראות הרשות לניירות ערך.

5. חברות בינוניות: בישראל מאות חברות המספקות מוצרים ושירותים משמעותיים למשק (למשל: חברות שינוע והובלה, בתי דפוס גדולים, אפליקציות מידע ומסחר, תאגידי מים). חלקן מחוברות רשתית לגופים הגדולים, משפיעות על יכולת התפקוד המשקית, וחשופות למידע קניין רוחני ופרטי נרחב. נכון יהיה לשקול לפתח תפיסה לאומית רחבה לגופים אלו שהיא מעבר למאמצי ההנחיה וההדרכה כיום, שתכלול תקינה ברורה ורגולציה מחייבת וגוף מרכזי לייעוץ, סיוע ואכיפה.

6. עסקים קטנים: עשרות אלפי העסקים הקטנים, שחלק לא מבוטל מהם מהווה ספק לגופים גדולים ומתוכם כאלו הנגישים למידע רגיש מאוד (למשל: משרדי עורכי דין וראיית חשבון), צריכים גם הם לזכות לתפיסה כוללת בניהול גוף מרכזי ובביצוע מבוזר הפורסת מעליהם מטריית הגנה, ומנגישה להם שירותי הגנת סייבר שאין ביכולתם לתחזק בעצמם.

7. ולבסוף, הציבור כולו ('הלקוחות'): ב'רשת אספקה' בשונה מ'שרשרת אספקה' הלקוחות צריכים להילקח בחשבון, מכיוון שחלק לא מבוטל מהם הם בעצמם ספקים של תאגידי וחברות גדולות, יש להם נגישות למערכות המידע של גופים אלו, והם יכולים להוות אמצעי לתקיפות סייבר נרחבות (למשל תקיפות DNS). תפיסת מענה המעלה את רמת 'היגיינת הסייבר' של הציבור הרחב על-ידי הנגשת מידע ואמצעים הנה חלק אינהרנטי מראייה של 'רשת אספקה'.

בדיון שהתקיים ב-18 ביוני 2023 בהובלת מערך הגנת הסייבר, הורה ראש הממשלה לשרים, על-פי הודעת הסיכום: "להיערך לחיזוק התשתיות החיוניות ולקדם את רגולציית הגנת הסייבר על הגופים שבאחריותם. בנוסף, ראש הממשלה הורה

להתחיל בקידום חוק הגנת סייבר, אשר ישען על פרקטיקה בין-לאומית אל מול: 1. רגולציה על תשתיות חיוניות. 2. תו תקן לכל המשק".

הסוגיה לדיון: האם אסטרטגיית הסייבר הלאומית יכולה להסתפק בטיפול בתשתיות חיוניות ולצד זאת לבנות תו תקן כללי לכל המשק, או שעליה להעמיק בפילוח כלל המעגלים שתוארו להלן ולתפור מענה - כולל תשומות לאומיות בעיקר מול התאגידים הבין-לאומיים - ובמענה לכל אחד מהם?

המלצה: במסגרת התהליך האסטרטגי נכון יהיה למפות את המעגלים שלהם הגופים הממשלתיים והעסקיים מתקשים במתן מענה הגנתי עצמאי, ושלפעילות המדינה יכולה להיות תרומה משמעותית בסגירת הפערים ולתעדף את המענה לפתרונן. למשל, הרמה המדינתית היא זו שיכולה להציב דרישות בפני תאגידים בין-לאומיים ולהוביל את תהליך בניית 'הגיינת סייבר' סבירה של הציבור הרחב.

#### סוגיה 4 - הגישה הבסיסית של מערך הגנת הסייבר

אין ברצוני להיכנס לסוגיית החקיקה והאסדרה הרגולטורית של מערך הסייבר הלאומי. נהרות של דיו נשפכו על הסוגיה, במיוחד סביב ובעקבות הכישלון בדיון סביב תזכיר חוק הגנת הסייבר ומערך הסייבר הלאומי מ-2018. הלקח העיקרי מההתנהלות אז הוא, להבנתי, הצורך לשתף את הארגונים הגדולים במשק ואת קהילת מומחי הסייבר בתהליך. מכיוון שטיטות הצעת החוק החדשה כבר מופצות להתייחסות בקרב קבוצה מצומצמת של מומחים וללא שקיפות רחבה, לא בטוח שלקח זה מיושם.

מתוך מכלול ההיבטים האפשריים באשר לגישה הבסיסית של מערך הסייבר הלאומי, יש שניים שבעיני נכון לקיים עליהם דיון עמוק, מעבר לאסדרה החוקית. הראשון הוא זהותו של המערך כגוף. הוא מגדיר את עצמו בעמוד הבית כ"גוף ממלכתי, מבצעי וטכנולוגי האמון על הגנת מרחב הסייבר הלאומי ועל קידום וביסוס עוצמתה של ישראל בתחום". מערך הסייבר יכול להיות כל אחד מהמודלים הבאים:

1. ארגון ביטחוני-מבצעי שמטפל באחד מהאיומים על מדינת ישראל בדומה לצה"ל, המוסד והשב"כ בכל הנוגע לאיומים ביטחוניים אחרים.
2. ארגון אכיפת חוק העוסק בפשיעה במרחב הסייבר בדומה למשטרה ולגופי אכיפה אחרים (הרשות להגנת הפרטיות, רשות המיסים בתחומה ועוד).

3. ארגון עבודת מטה ואסדרה ממשלתי המנחה את משרדי הממשלה כיצד להפעיל את היכולות הרגולטוריות שלהם בתחומי עיסוקם להבטחת הגנת הסייבר בדומה - לא בהלימה מלאה - למטה לביטחון לאומי.
4. ארגון אסדרה לאומי היוצר, מנחה ואוכף רגולציית הגנת סייבר: המערך כבר ירש במסגרת תיקון החוק להסדרת הביטחון בגופים ציבוריים ב-2016 מהשב"כ - בשיתוף פעולה ובהנחייה שלו - את היותו קצין מוסמך לפעולות אבטחת מידע לכחמישים גופים המוגדרים תשתית מדינה קריטית המופיעים בתוספת החמישית לחוק. על-פי סיכום שנת העבודה 2022 של המערך, רשימת הגופים המונחים מעודכנת מדי תקופה על-ידי ועדה בין משרדית בראשות ראש מערך הסייבר הלאומי. ההנחיה והבקרה של גופים אלו מבוצעים על בסיס תו"ל רימון הכולל חמש מדרגות ומעל 900 בקרות בסה"כ.
5. גוף אכוונה ומידע לאומי בתחום הגנת הסייבר בדומה לרשות הלאומית לבטיחות בדרכים בתחומה.

ישנם מודלים נוספים אפשריים, דוגמת בנק ישראל, שהנו תאגיד שמטרתו המרכזית לשמור על יציבות המחירים, אך אלו פחות רלבנטיים.

בהמשך לדיון על מעגלי ההגנה הלאומיים ניתן להגיד שלכל אחד מהמעגלים ועם האתגרים עימם מערך הגנת הסייבר צריך להתמודד על מנת לממש את ייעודו ניתן לתפור תמהיל שונה של מאפיינים. למשל, אלו מול תשתיות לאומיות קריטיות המערך כבר מבוסס כארגון אסדרה, הנחיה ואכיפה לאומי. אל מול משרדי הממשלה וגופים גדולים במשק המפוקחים על-ידם נכון שיתפקד כארגון עבודת מטה ואסדרה ממשלתי. אל מול עסקים קטנים והציבור כולו נכון שיעבוד בעיקר כגוף אכוונה ומידע לאומי.

הבעיה העיקרית בהתנהלות כזו היא שעלולות להיות סתירות בין התפקודים השונים, שיקשו על שיתוף הפעולה מצד הגורמים במעגלים השונים. למשל, אם המערך ייקח לעצמו סמכויות של ארגון ביטחוני-מבצעי או ארגון אכיפת חוק בעת טיפול באירוע סייבר בארגון אזרחי, הוא עלול לאבד מיכולתו להוות גוף אסדרה ממשלתי המנחה את הרגולציה, מכיוון שיכולת הפעולה והאכיפה הישירה עלולה לפגוע ביחסים בין הרגולטור לאותו הארגון האזרחי.

בנוסף, בעוד שבסיוע בהגנת הסייבר למשק האזרחי מערך הסייבר הלאומי ויחידות הגנת הסייבר במשרדי הממשלה השונים הם גורמי מענה ייחודיים ולעיתים בלעדיים; הרי שבהיבטים הביטחוניים, המבצעיים והאכיפתיים יש במדינת ישראל גופים ותיקים מהם, שכבר עוסקים בטיפול באתגרים. דבר זה אמור לאפשר למערך לעסוק בפערים העיקריים במשרדי הממשלה ובמשק האזרחי ופחות בהיבטים ביטחוניים-מבצעיים.

הסוגיה לדיון: מה הוא התמהיל המיטבי של המודלים האפשריים של ארגונים ממשלתיים (ביטחוני-מבצעי, אכיפת חוק, אסדרה ממשלתית, אסדרה לאומית, או גוף אכוונה) שהמערך יכול לאמץ לעצמו באופן שיאפשר לו למלא את תפקידיו בצורה מיטבית ברמות השונות - ההגנה, המוכנות לאירוע, ניהול האירוע ופעולות האכיפה והתגובה נגד מבצעי האירוע - ואל מול כלל המעגלים שתוארו בהתאם לחשיבותם?

ההיבט השני שנכון לעסוק בו הוא כפיפותו של מערך הסייבר הלאומי. דיון זה נמצא גם הוא בזיקה לזהותו של המערך כגוף. מערך הסייבר - על גלגליו השנים - צמח בתוך משרד ראש הממשלה ובכפיפות ישירה לראש הממשלה (למעט תקופה שהוכפף לכאורה לשר הפועל תחת ראש הממשלה). בשלב ההבשלה היו לכך יתרונות מהותיים, ואלו עדיין מתקיימים. יכולת הפעולה העצמאית, הגיבוי של ראש הממשלה והמעמד האקס טריטוריאלי למשרדי הממשלה הם מאפיינים שלאורך השנים עמדו לטובת המערך.

עם זאת, אין זה טבעי שהעיסוק בהגנת הסייבר הלאומית תהיה בהכרח כפופה ישירות לראש הממשלה, ובתהליך ההתמסדות הדבר אף עלול להגדיל את החסרונות על פני היתרונות: ראש המערך אינו שווה בין שווים מול השרים, ולכן, אינו יכול להנחות את המשרדים ללא גיבוי מלא של ראש הממשלה. העובדה שלא חוקק עדיין חוק הגנת סייבר לאומי, מצביעה על הקושי לגלם את הכפיפות הישירה אליו לתהליכי הסדרה ואסדרה. הקשב של ראש הממשלה למערך - במיוחד להיבטים במכלול העשייה שלו - מוגבל, ועשוי להקשות על קידום יוזמות של המערך הנדרשות לתמיכתו. היותו מערך עצמאי גם מרחיקה אותו ממחוזות של שיתוף פעולה טבעי כמו ביטחון, ביטחון פנים וקידום המחשוב הלאומי.

ניתן לחשוב, גם תוך הסתכלות על מדינות אחרות, על כפיפות שונה למערך: המשרד לביטחון לאומי, משרד העוסק בחדשנות טכנולוגית ובמחשוב הלאומי, משרד האוצר או משרד הכלכלה. חלק מתהליך ההתבגרות והנירמול של הטיפול בהגנת הסייבר הלאומית - וניהול הממשקים בין הארגונים השונים העוסקים בה - יכול להיות שילוב מערך הגנת הסייבר לתוך מעטפת נכונה של משרד ממשלתי.

הסוגיה לדיון: האם לא נכון לקדם בהסתכלות ארוכת טווח שילוב של מערך הגנת הסייבר במשרד ממשלתי שיקצה לו קשב, ממשקים ולעיתים משאבים, שהוא אינו יכול לקבל ממקומו העצמאי כמערך תחת ראש הממשלה?

המלצה: בהחלטות על התמהיל המיטבי של מאפייני מערך הסייבר הלאומי וכפיפותו נכון לקחת בחשבון את שיטות ההשפעה האפקטיביות ביותר של גופים ממשלתיים על הנעשה במשרדי ממשלה ובמגזר העסקי. נכון שמערך הסייבר הלאומי ויחידות הגנת הסייבר במשרדי הממשלה יתמקדו בהגנה על גופים אלו, ולא יעסקו בהיבטים ביטחוניים, מבצעיים ואכיפתיים המטופלים על-ידי ארגונים אחרים. במסגרת זו, על פניו נראה כי השילוב בין אסדרה, רגולציה ואכיפה שלהם הוא האפקטיבי ביותר.

#### **סוגיה 4 - במגזר הממשלתי**

לאורך השנים התקשה מערך הגנת הסייבר הלאומי לפעול לקידום הגנת הסייבר במשרדי הממשלה הלאומיים. תהליך הטמעת תהליכי וגופי הגנת סייבר ואסדרה במשרדי הממשלה ורשויות לאומיות נמשך שנים רבות, ועדיין לא הגיע לנקודה המיטבית.

ביטוי לכך הייתה העובדה שבשנים קודמות ההתייחסות להיבטי הגנת הסייבר במסמך עיקרי תוכניות העבודה של משרד הממשלה הייתה ספורדית עד בלתי קיימת כלל. במסמך לשנת 2023 ניכר שינוי המייצג עליית מדרגה בהתייחסות של משרדי הממשלה לסוגיה. חוץ ממערך הסייבר הלאומי, סוגיית הסייבר נכללת בעיקרי התוכניות של עוד עשרה מתוך 59 המשרדים והגופים המופיעים בתוכנית. אלו מהווים 18% מגופי הממשלה, שיש לומר שעבור חלק מהם סוגיית הגנת הסייבר לא אמורה להוות היבט משמעותי בפעילותם. במסגרת הגופים שכן מכלילים את הגנת הסייבר בעיקרי תוכנית העבודה ניתן לציין משרדים משמעותיים ורלבנטיים לסוגיה כמו משרד האנרגיה והתשתיות, המשרד לביטחון

לאומי, משרד החדשנות, המדע והטכנולוגיה, מערך הדיגיטל הלאומי ומשרד התקשורת. יש לציין את משרד המודיעין שבתוכנית העבודה שלו מופיעים יעדים של חקיקה ורגולציה בתחום הסייבר בשיתוף מערך הסייבר הלאומי.

לעומת זאת, עבור כמה משרדים ממשלתיים חשובים להקשר זה הסייבר אינו מתעלה לכדי סעיף מפתח בתוכנית העבודה. מגדיל לעשות משרד הבריאות, שהארגונים הקשורים בו ספגו מתקפות סייבר בשנים האחרונות מהן שתיים שהתפתחו לאירועי סייבר מהותיים. מנכ"ל המשרד קובע בפתיח לתוכנית, כי "ברמה העולמית ישנם אתגרים חדשים כמו עלייה משמעותית באיומי סייבר ובתקיפת ארגוני בריאות בתחומים אלו", אך סוגיית הסייבר לא מופיעה כיעד בתוכנית העבודה של המשרד. משרדים נוספים שהסייבר ראוי היה שיקבל ביטוי בעיקרי תוכנית העבודה שלהם הם משרד התחבורה, שבו לפגיעת סייבר עלולות להיות משמעותיות קטלניות; משרד הפנים שאחראי על הרשויות המקומיות שבהן מצב הגנת הסייבר - על-פי דוחות מבקר המדינה - אינו טוב בלשון המעטה; ומשרד החינוך שמחזיק - הוא והארגונים הכפופים לו - מידע אישי רב ורגיש על ילדים ובני נוער.

למרות ההתקדמות המשמעותית, הסדרת גופי הגנת סייבר במשרדי הממשלה כולל חמ"לי סייבר העובדים בשיתוף פעולה ובשיתוף עם מערך הסייבר הלאומי, היבטי הטיפול בהגנת הסייבר במשרדי הממשלה עדיין אינם זוכים בחלק מהמקרים לקשב ולמשאבים הראויים להם.

הסוגיה לדיון: כיצד ניתן לקדם את היבטי הגנת הסייבר במשרדי ממשלה נוספים מעבר לאלו שכבר ביצעו את קפיצת המדרגה (משרד האנרגיה והתשתיות, משרד התקשורת ועוד), ושהגנת הסייבר בהם צריכה לזכות לקשב ולמשאבים מעבר לאלו הניתנים כיום (משרד הבריאות, משרד התחבורה, משרד הפנים, משרד החינוך ועוד)?

המלצה: הגברת המעורבות של מערך הגנת הסייבר ודחיפת פעילות ההגנה בכל משרדי וארגוני הממשלה - ובהמשך להסדרה ברורה של ייעודו ותפקידיו בתחום ההגנה - צריכה להיות יעד מרכזי באסטרטגיה על-פי תיעודו ברור בדגש על הבריאות, התחבורה, הפנים (הרשויות המקומיות) והחינוך.



## סוגיה 4 - מול המשק האזרחי

הגישה של המשק האזרחי כלפי מערך הגנת הסייבר הלאומי עדיין מתאפיינת בחשדנות. חברות עסקיות מתקשות לזהות את הרווח המובהק משיתוף פעולה עמו, בעוד המחירים בקשב ובמשאבים מולו מוחשיים יותר. הדרך הטובה ביותר לרתימת ארגונים אלו עשויה להיות באמצעות סיוע במקומות שהמדינה יכולה לעשות דברים שהארגונים אינם חזקים מספיק בשביל להשיג. דוגמאות:

1. טיפול לאומי ב'שרשרת האספקה': כפי שתואר להלן במעגלי הגנת הסייבר הלאומיים, יש מספר ארגונים בין-לאומיים גדולים וחברות ישראליות משמעותיות שהן ספקיות שירותים של מאות הארגונים הגדולים בישראל. דוגמאות בולטות הם העננים של ו-Azure והמערכות של ו-Salesforce ו-SAP הנמצאים כיום כמעט בכל ארגון משמעותי. לצד זה ניתן לציין גם חברות ישראליות כמו חיל"ן או מל"מ שכר שמחזיקות את חישוב השכר של רוב או אפילו כמעט כל הארגונים. הם הפכו גם בהיבט הסייבר לצווארי הבקבוק של המשק הישראלי. המדינה יכולה לסמן את הספקים הרחוביים העיקריים ולפעול מולם בעצמה כאילו היו תשתית קריטית, ובכך להקל מאוד על הגנת הסייבר הארגונית.

דוגמה שלילית המבהירה צורך זה הייתה סירוב המדינה לטפל מול חברות התקשורת בהקשחה משמעותית של הנתבים הביתיים, בשעה שכל המשק עבר לעבודה מרחוק בתקופת הקורונה, והנתבים הפכו לרכיב סיכון מרכזי להתחברות לרשתות ארגוניות. כפי שצוין, בשנתיים האחרונות ביצע משרד התקשורת בשיתוף עם מערך הסייבר הלאומי שינוי מהותי במדיניותו בסוגיות כאלו.

2. רגולציה מקדמת שינוי חיובי: רגולציה יכולה להיות מכשיר מצוין להעלאת רמת הגנת הסייבר של מגזר אזרחי. היא מחייבת את הארגון - לעיתים תוך התמסרות מרצון - לעסוק בסוגיות שבשטף העיסוק בשיקולים העסקיים לא זוכים לטיפול נאות. עם זאת, דרישות פרטניות מדי - שמשפיעות לרעה על הרכיב הטכנולוגי והעסקי ולא מותירות שיקול דעת לארגונים - עשויות להרחיק ולחבל בשיח וברמת הגנת הסייבר של הארגונים ולא לשפר אותה. אם בכירי הארגון חושבים שהמדינה פולשת לליבת השיקולים העסקיים שלו והרגולטורים פועלים מתוך מוטיבציה של 'כיסוי תחת' ומנצלים את

יכולות הארגון לצרכיהם, הם יצמצמו את השיח עמם, ויפעלו במאפיינים של ההשקעה המינימלית הנדרשת על מנת 'לעבור' את הדרישות. הדבר בא לידי ביטוי, למשל, בדרישות דיווח מפורטות מאוד וחודרניות על אירועי סייבר ואף על חשד לאירועים; דרישות ישנות ואנכרוניסטיות שלא מעודכנות בהתאם להתפתחות הטכנולוגית; ויכולת אכיפה והשפעה על החלטות הארגון הנתפסת כדרקונית וחודרנית מדי, וראה, כאמור הביקורת הרחבה על תצהיר חוק הסייבר מ-2018.

התנהלות חכמה של הגורמים הממשלתיים יכולה לייצר את האיזון הסביר בין הנכון ללא נכון, לקדם את הגנת הסייבר ולא להכביד עליה. הדוגמה המובהקת בישראל היא הבנקים והשינוי החיובי שעברו מאז כניסתה לתוקף של הוראת ניהול בנקאי תקין 361 בתחום הגנת הסייבר ב-2015 והוראות משלימות נוספות מאז. אלו מנוסחות כך שהן מותירות לבנקים שיקול דעת בתחום היישום, ומאפשרות להם לפעול לפי המאפיינים הפרטניים של הבנק. מנגד, הטמעת תו"ל רימון בתשתיות קריטיות זוכה גם היא להיענות גבוהה יחסית, משום שהיא מלווה בהנחיה צמודה, ומותירה לארגון שיקול דעת ביישום. ניתן לצרף לציות לרגולציה גם שיטות של תימרוץ כספי או מוניטיבי; למשל, משרד ההגנה האמריקני מעניק בכל שנה תעודות הצטיינות לחברות שמתבלטות בעמידה בדרישות הביטחון שלו.

3. 'שמיכת הגנה': למדינה יש יתרונות פוטנציאליים מובנים בתחום המודיעין, ההתרעה, ידע ויכולות בתחום הסייבר וניטור צווארי בקבוק תשתיתיים לאומיים ויכולת תגובה בכלים אכיפתיים-חוקיים וביטחוניים-מבצעיים, שיכולים להוסיף שכבת הגנה נוספת חוץ ארגונית. ארגונים רבים ישמחו לקבל אותה מהמדינה במיוחד במענה לתרחישי קיצון, שבהם הם נתקפים על-ידי תוקף מעצמתי, שנדרשים משאבי עתק על מנת להגיע לרמת הגנה, שתיתן מענה לאיום מצדו.

מימוש של 'שמיכה' כזו מחייב את הגופים המדינתיים - בדגש על מערך הגנת הסייבר - למחויבות לפעולה רציפה ולרמת ולאיכות מענה המשרת את צרכי הארגונים, כאמור, במיוחד מול מתארי תקיפה ברמה גבוהה מאוד ובפוטנציאל נזק חריג. בבואו לממש את המטרה של 'הקמת כיפת סייבר לאומית' רצוי שמערך הגנת הסייבר יתמקד ביכולת המענה לסוגי

איומים אלו תוך בניית גשר בין המשק האזרחי לבין הארגונים הביטחוניים. אחד האתגרים המורכבים בהקשר זה הוא לתווך מידע - בעיקר התרעות - ממקורות מודיעין מסווגים ורגישים מאוד לארגונים האזרחיים, על מנת שאלו ייתנו מענה מותאם לאיומים הן כלליים והן ממוקדים.

4. טיפול במחסור בכוח האדם: יש מחסור עמוק באנשי הגנת סייבר בארגונים. אנשי טכנולוגיה טובים מעדיפים חברות טכנולוגיה וסטארט-אפים בשל הכסף והעיסוק בפיתוח טכנולוגי, אבל רוב הגנת הסייבר נעשית בארגונים וחברות גדולים. חברה גדולה נזקקת לעשרות אנשי סייבר במקצועות שונים - מיישום טכנולוגי ועד טיפול בתהליכי הגנת סייבר, ורוב החברות במשק מתקשות למלא את השורות במערכי הגנת הסייבר שלהם. מערך הסייבר הלאומי יכול לסייע באמצעות תוכניות לאומית לגיוס ולהכשרה של מגני סייבר. משרד המודיעין הציב לעצמו יעדים בתחום זה בשיתוף המערך: "משרד המודיעין פועל להגדלת ההון האנושי המיומן בתפקידי סייבר, בהגדלת התעסוקה של אוכלוסיות שבייצוג חסר במשרות אלה (נשים, חרדים, ערבים, תושבי פריפריה, חיילים קרביים משוחררים), וכן בצורך לקדם תוכניות חשיפה והתנסות בתחום בגיל הצעיר והמשך בתוכניות התמחות בגיל התיכון".

בשנים האחרונות עוסק מערך הסייבר הלאומי באסדרת מקצועות הגנת הסייבר כולל ברגולציה מחייבת. זהו תהליך חשוב, שיקדם את היקף המועסקים בעלי הידע בתחום הגנת הסייבר, ולא ייצר צוואר בקבוק של תהליכי הסמכה מורכבים ופסילת בעלי מקצוע טובים החסרים 'השכלה פורמלית'.

5. עבודה עם חברות שירותי הגנת הסייבר: מכפיל כוח משמעותי בהגנת המרחב האזרחי הוא החברות שעוסקות במתן שירותי הגנת סייבר מייעוץ בתחומים שונים, דרך סקרים ומבדקי חדירה, יישום תהליכים טכנולוגיים בארגונים ועד מענה חקירה ופורנזיקה בהתרחש אירוע ושירותי הגנת סייבר מלאים בתשלום (CisoaaS, MSSP). למען הגילוי הנאות ייאמר, שהכותב מחובר לחלק מחברות אלו, ולשירותים שהן מעניקות. חברות אלו צריכות להיתפס על-ידי מערך הגנת הסייבר כזרוע ארוכה שלו. השיח בין הצדדים הוא לעיתים חשדני, ונובע מתקדימים היסטוריים שבהם המערך ניצל את

הידע של החברות ללא תמורה, או העדיף חברות ייעוץ בינלאומיות גדולות על פני חברות מקומיות המכירות לעומק את צרכי המשק הישראלי. נכון לבחון הקמת מנגנון - בין היתר פורום מנהלים - של שיח מתמיד בין המערך לחברות אלו.

הסוגיה לדיון: כיצד יכולה אסטרטגיית הגנת הסייבר הלאומית להביא לתהליכי שיתוף הפעולה המיטביים עם המשק האזרחי, בין היתר, על ידע מימוש התהליכים שתוארו להלן ונוספים?

המלצה: נכון שפתרון המצוקות הרוחביות - בדגש על המחסור בכוח אדם מיומן לתחום הגנת הסייבר - יהיה מנוע מרכזי במערכת היחסים בין מערכת הסייבר הלאומי לבין המשק האזרחי.

### סוגיה 5 - מאמצים בתחום הגנת הסייבר הלאומית

בחלק אחרון זה ברצוני להתייחס באופן פרטני למספר מאמצים בתחום הגנת הסייבר הלאומית.

הכשרות הגנת סייבר: בישראל קיימת תעשייה נרחבת באוניברסיטאות, במכללות אקדמיות ובמכללות מקצועיות ייעודיות להכשרה למקצועות הסייבר.

הסוגיה הראשונה הקשורה בהן היא ההיקף. במשק האזרחי קיים מחסור בכוח אדם מיומן בתחום הגנת הסייבר. הדבר מקבל יתר דגש במעבר של משרדים וארגונים ממשלתיים וחברות גדולות להתבססות על ענן ציבורי ובמסגרת זו המהלך הלאומי להקמת נימבוס. סוגיה נוספת היא השתנות תהליכי הפיתוח של מערכות מחשוב, הדיגיטציה המואצת והאוטומציה של ההגנה המחייבים מקצועיות מתקדמת יותר של אנשי ההגנה. ממשלת ישראל - ובתוכה מערך הגנת הסייבר כמנוע מרכזי לתהליך - צריכה להרחיב ולהאיץ את תוכניות ההכשרה למקצועות הגנת הסייבר הרלבנטיים, למשל, תוך הרחבת שיתוף הפעולה עם חברות הטכנולוגיה הגדולות, מוסדות אקדמיים וחברות השירותים והייעוץ.

הסוגיה השנייה הקשורה בהן היא האסדרה. חלק לא מבוטל מהכשרות אלו מבוצע על בסיס סטנדרטים והסמכות בין-לאומיים. קיים צורך לוודא שבוגרי ההכשרות הנם בעלי ידע מספק על מנת להתחיל לעבוד באופן מעשי במקצועות השונים. לצורך כך מקודם מזה מספר שנים תהליך אסדרה של מקצועות הסייבר. יחד

עם זאת, ההתקדמות הטכנולוגית משפיעה על מקצועות הסייבר, ורוב תהליך ההתאמה לצרכי האמת מבוצעים לאורך זמן בלמידה עצמית של בעלי המקצוע עצמם או של הארגונים. בנוסף, חלק מהעיסוק בסייבר מחייב חשיבה יצירתית והסתגלות המנותקת מידע הנרכש בתוכניות לימוד 'קשיחות' יחסית. כפועל יוצא נדרש לבחון את התמהיל בין אסדרה של ההכשרות והקפדה על דרישות הסמכה של בעלי מקצוע טרם קליטתם במקומות העבודה לבין הצורך לשמר גמישות חיונית, שאינה מכוסה על-ידי אסדרה פורמלית לתהליכי למידה ובנייה של פתרונות ראשוניים ויצירתיים.

עידוד לאומי של מחקר ופיתוח (מו"פ) ופיתוח התעשייה בתחום הסייבר: מאז שנות התשעים ובגלגוליו הראשונים של מערך הסייבר הלאומי השקיעה מדינת ישראל לא מעט בקידום מו"פ ויזמות עסקית בתחום הסייבר. עידוד המו"פ בתחום הסייבר הוגדר כיעד במיזם הקיברנטי מ-2011. באסטרטגיית הסייבר הלאומית מ-2017 מופיע, כאמור, מאמץ על של "מחקר, פיתוח ויישום של יכולות וטכנולוגיות הגנה מדינתיות". יזם הסייבר אלון ארביץ, בספרו 'ההגנה הטובה ביותר' על תעשיית הסייבר הישראלית, מנתח מאמצים אלו ומסכם (ע' 229): "קשה להפריז בערכם של המאמצים של מדינת ישראל לייצר סביבה נוחה לתעשיית הסייבר, אך חשוב לדייק ולראות מה מתוך כל המאמצים הללו באמת מקדם את התעשייה... חברות הסייבר זקוקות בעיקר לחופש שייתן ליוזמה הפרטית, לכוח האדם האיכותי ולהון שזורם למדינה לפעול יחד... הקלות המס והרגולציה הנמוכה מועילות פי כמה וכמה מהניסיון ליצור מוקד סייבר נוסף בבאר שבע... הצמיחה תלויה לא במה שהמדינה תעשה, אלא בעיקר במה שהיא לא תעשה".

תוכנית העבודה של מערך הגנת הסייבר לשנת 2023 צנועה מקודמותיה בקידום מו"פ ומוצרי הגנה, ומגדירה ארבעה תחומים ממוקדים לקידום המענה הטכנולוגי: הגנת שכבת הפרוטוקול, תשתית להנגשת שירותי הגנת סייבר, תשתית להערכת רמת החוסן של המשק ויכולת ניטור על בסיס ענן ציבורי. מדובר בשינוי דרך הסתכלות מקידום כללי של הטכנולוגיה והתעשייה של הגנת הסייבר למתן מענה ממוקד על-פי ניתוח הצורך. לכך מצטרף הצורך של מדינת ישראל לפרוץ דרך בתחומים קריטיים אחרים דוגמת מחשוב קוואנטי, בינה מלאכותית ואנרגיה חלופית. כל אלו מצביעים על רצון וצורך לתחם את מאמצי העידוד הלאומיים בתחום הגנת הסייבר.

המיוצב הבין הלאומי והיקפי שיתוף הפעולה: בסיכום שנת העבודה 2022 הציג מערך הסייבר, כי הוא מקיים קשר מבצעי עם 33 מדינות, ושותף פעיל בשלושה פורומים רב-לאומיים. ברשימת המדינות מופיעות חלק ממעצמות הגנת הסייבר המובילות בעולם: ארצות הברית, בריטניה, גרמניה, אוסטרליה ועוד. מהצד האחר חסרות ברשימה מדינות מובילות בתחום ההגנה דוגמת צרפת והולנד. בהקשר של קידום מדיניות החוץ של ישראל ('דיפלומטיית סייבר') מופיעות ברשימה מדינות 'הסכמי אברהם' איחוד האמירויות ומרוקו ומדינות מפתח עבור מדיניות החוץ הישראלית דוגמת הודו, יפן, יוון וקפריסין ועוד. עם זאת בהסתכלות על הרשימה ניתן להגיד, שחלקה מייצג מימוש של הזדמנויות לשתופי פעולה יותר מאשר תוכנית סדורה המציבה יעדים ברורים הן בהיבטי צרכי הגנת הסייבר והן בהיבטי יעדי מדיניות החוץ, ומבקיעה אותן.

בניית שיתופי פעולה הנם מאמץ תומך חיוני למאמצי הליבה של הגנת הסייבר. הוא יכול להקנות תמורות מהותיות בתחומי מאמץ ההגנה המבצעי, שיתוף פעולה טכנולוגי, למידה הדדית והשפעה ישראלית נדרשת מאוד על גיבוש נורמות בין-לאומיות בתחום הסייבר. 'דיפלומטיית סייבר' הנה רכיב משמעותי גם בסל הכלים של מדיניות החוץ הישראלית. עם זאת, נכון לתחם ולמקד את המשאבים המושקעים במאמץ זה באמצעות תוכנית ברורה עם סדרי עדיפויות קשיחים וגמישות מסוימת להזדמנויות. סוגיה נוספת שחשוב לבחון בהקשר הבין-לאומי, ושמעסיקה מדינות מובילות רבות בעולם בעקבות לקחי המלחמה באוקראינה, הינה בניית יכולת לאומית ישראלית נצורה - בשיתוף המגזר האזרחי - לפרוס מעטפת הגנה למדינה הנכנסת למצב מלחמה או עימות סייבר עם מדינה אחרת.

תמהיל הלימוד ממדינות אחרות אל מול תפירת מענה לאופי הישראלי: נכון לייבא מה שנקרא פרקטיקות מיטביות של הגנת הסייבר מהעולם. יש לנו הרבה מה ללמוד בעיקר בהיבטי שיטתיות וניהול מיטבי של מאמץ ההגנה. יחד עם זאת, חלק מהדרישות בארצות הברית ובאירופה מבוססות על גישה בסיסית מתאימה יותר לתרבות הלאומית העסקית של מדינות אלו - תרבות של ציות ותהליכים פורמליים. זו אינה לוקחת בחשבון רכיבים של האופי הישראלי, שמצד אחד נותן יותר מקום ליצירתיות ולשונות, ומהצד האחר נזקק לגבולות ברורים. בישראל עדיפה חומת הפרדה בין מסלולים - קרי, הגנת סייבר המבוססת על מגבלות טכנולוגיות מוכתבות, על פני ציור של פסי הפרדה על הכביש - קרי, התבססות

על תהליכים של פעולה אנושית. דוגמה לסוגיית ההתאמה לאופי ישראלי מהווה ההבדל בין התקבלות נב"ת 361 בבנקים לבין ההטמעה של תורת ההגנה בארגונים גרסה 1.0, שהפיץ מערך הגנת הסייבר באפריל 2018. בעוד הנב"ת קצר בהיקפו, ומותר לא מעט שיקול דעת וגמישות לדרך היישום של הבנקים, הרי שתורת ההגנה, ובעיקר האקסל המפורט הנלווה עליה, מפרטים מאות רבות של צעדים שעל הארגון לבצע, שקשים הרבה יותר לעיכול וליישום.

על-פי ההודעה לעיתונות על דיון ראש הממשלה ב-18 ביוני 2023, הציג ראש מערך הסייבר הלאומי השוואה בין-לאומית, לפיה "ישראל נמצאת בפער ברגולציה הסייבר אל מול מדינות מתקדמות בעולם, בהן גרמניה, אוסטרליה, בריטניה, ארה"ב וכן האיחוד האירופי, שם נקבעו בחוק עקרונות של חובת ניהול הסיכון על ארגונים חיוניים, חובת דיווח על אירועי סייבר, סמכויות פיקוח ואכיפה לרגולטורים וחוק מוסדר בנושא הגנת סייבר". אין ספק שהשוואת המצב בישראל למצב בעולם היא כלי משמעותי בחשיבה על אסטרטגיית הגנת הסייבר, אך בתהליך קביעת העקרונות חשוב שהמודלים החיצוניים יסוננו בקפידה ויותאמו למאפיינים הישראליים הייחודיים.

הסדרת סוגיית מס רכוש: העיסוק בביטוח סייבר התרחב משמעותית בעשור האחרון, ואף מהווה במקרים מסוימים דרישה רגולטורית. בעיה מרכזית בתחום הכיסוי הביטוחי לאירועי סייבר בעולם ובארץ הנה, שישנה מגמה להחריג תקיפות סייבר מדינתיות (state cyber operations) בביטוחים אלו. כפועל יוצא ארגונים שנראה כי נתקפו על-ידי גורמים מדינתיים, אינם זכאים לשיפוי במסגרת הכיסוי הקיים. מדובר בסוגיה שיש בה עיסוק נרחב בעולם הביטוח, ומכיוון שחובת ההוכחה לגבי זהות התוקף הנה על חברות הביטוח, הן גוררות גורמי הגנת סייבר לאומיים לתוך ההתדיינות המשפטית. בישראל המצב מורכב יחסית לעולם, משום שהמשק האזרחי נתקף במובהק על-ידי איראן, חזבאללה וחמאס, ונגרמים לו נזקים מסוגים שונים כתוצאה מכך. הכתובת לשיפוי על נזקים אלו הנה מנגנון מס רכוש, אולם במדינת ישראל אין תהליך מוסדר של ייחוס התקפת סייבר לגורם מדינתי או טרור והפניית הנפגעים לקבלת פיצוי מהמדינה. ניכר שאת הסוגיה הזו יש להסדיר, ומערך הסייבר הלאומי ראוי שיעסוק בה גם כמאפשר מרכזי לשימוש בביטוחי סייבר כרכיב תורם במענה לאירועים.

הסוגיות לדיון: עד כמה ובאיזה צורה צריך מערך הסייבר הלאומי וגורמים לאומיים לעסוק במאמצי הגנת הסייבר השונים?

המלצה: בראיית הכותב יש להרחיב מאוד את העיסוק בהכשרת כוח אדם מיומן להגנת הסייבר עבור משרדי הממשלה והמשק האזרחי ולהגמיש את האסדרה בתחום זה; לעומת זאת ניתן לתחם ולצמצם את מאמצי העידוד הלאומיים בתחום מחקר ופיתוח לתחום הגנת הסייבר; נכון למקד ולתחם את המאמץ לקידום שיתופי הפעולה הבין-לאומיים בתחום הגנת הסייבר על-פי סדרי עדיפויות קשיחים יותר תוך גמישות מסוימת להזדמנויות כולל סיוע חירום למדינות מותקפות; את הלמידה והאימוץ של נורמות חיצוניות להגנת הסייבר נכון לסייג ולהתאים יותר למאפיינים הייחודיים של ישראל; וחשוב לבצע עבודה מטה לאומית לאסדרת פיצוי מס רכוש על אירועי סייבר מצד גורמי תקיפה לאומיים וארגוני טרור.

## סיכום

בנייר זה פורטו שאלות וסוגיות מפתח שראוי לייחד להם דיון בעת קביעת אסטרטגיית סייבר לאומית. הסוגיות נוסחו בכוונת מכוון בדרך של שאלות, ועל מנת לענות עליהן נדרשים תהליכי ניתוח המשכיים. לצד זאת צורפו כיוונים ראשוניים של המלצות לפעולה במענה לסוגיות אלו. מעבר להנחת הסוגיות לפתחו של תהליך גיבוש אסטרטגיית הגנת הסייבר הלאומית, נכון שגורמי אקדמיה, מחקר ויישום יעסקו בתהליכים לקידום מענה הגנת הסייבר הישראלי.



## Recent BESA Center Publications

### Mideast Security and Policy Studies

- No. 175 The Trump Peace Plan: Aiming Not to Make a Deal but to Make a Deal Possible, *Douglas J. Feith and Lewis Libby*, June 2020
- No. 176 The COVID 19 Crisis: Impact and Implications, *Editor: Efraim Karsh*, July 2020
- No. 177 Palestinian Activists at Human Rights Watch, *Gerald M. Steinberg and Maayan Rockland*, July 2020
- No. 178 Israel Versus Anyone: A Military Net Assessment of the Middle East, *Kenneth S. Brower*, August 2020
- No. 179 The EU and Israel as Genuine Strategic Partners, *Florin Pasatoiu and Christian Nitoiu*, August 2020
- No. 180 The Israel-UAE Peace: A Preliminary Assessment, *Editor: Efraim Karsh*, September 2020
- No. 181 The American Public and Israel in the Twenty-First Century, *Eytan Gilboa*, October 2020
- No. 182 Iran Behind the Scenes During the Second Israel-Lebanon War, *Raphael Ofek and Pesach Malovany*, November 2020 (English and Hebrew)
- No. 183 The Pentagon's UAP Task Force, *Franc Milburn*, November 2020
- No. 184 The Second Nagorno-Karabakh War: A Milestone in Military Affairs, *Uzi Rubin*, December 2020 (English and Hebrew)
- No. 185 Iran's Killing Machine: Political Assassinations by the Islamic Republic, *Ardavan Khoshnood*, December 2020
- No. 186 The Battle for the Soul of Islam, *James M. Dorsey*, January 2021
- No. 187 The Caspian Sea as Battleground, *James M. Dorsey*, February 2021
- No. 188 The Abraham Accords: Contrasting Reflections, *Shmuel Trigano*, March 2021
- No. 189 American Development of UAP Technology: A Fait Accompli?, *Franc Milburn*, March 2021
- No. 190 Should Israel Cooperate with the ICC? *Anne Herzberg*, March 2021
- No. 191 The Logic Behind the JCPOA—Then and Now, *Oded Brosh*, May 2021 (English and Hebrew)
- No. 192 Middle East Futures: Defiance and Dissent, *James M. Dorsey*, June 2021
- No. 193 ASMLA: An Empirical Exploration of an Ethno-Nationalist Terrorist Organization, *Arvin Khoshnood*, June 2021
- No. 194 The Laundromat: Hezbollah's Money-Laundering and Drug-Trafficking Networks in Latin America, *Emanuele Ottolenghi*, July 2021
- No. 195 The 2021 Gaza War: The Air Campaign, *Ehud Eilam*, July 2021 (Hebrew only)
- No. 196 The Radicalized Israeli Arabs, *Efraim Karsh*, August 2021
- No. 197 A New Palestinian Authority NGO Decree Might Halt US Aid to the West Bank and Gaza, *Dore Feith*, August 2021
- No. 198 Iran's Nuclear Program: Where Is It Going? *Raphael Ofek*, September 2021
- No. 199 The Nagorno-Karabakh Conflict: Roots and Consequences, *Galit Truman Zinman*, September 2021
- No. 200 Russia's War Against Ukraine - Impacts on Israeli Nuclear Doctrine and Strategy, *Louis René Beres*, April 2023
- No. 201 The War in Ukraine: 16 Perspectives, 9 Key Insights, *Eado Hecht, Shai Shabtai (Eds.)*, August 2023
- No. 202 The Oslo Disaster 30 Years On, *Efraim Karsh*, September 2023
- No. 203 National Cyber Strategy: Issues for Discussion, *Shai Shabtai*, January 2024